NAS System

User Manual

Revision 1.0

P/N: PW0020000000373

Table of Contents

PART 1 Hardware Components and RAID Controller

Chapter 1 Introduction

The NAS System

Companies are looking for cost-effective storage solutions which can offer the high performance, high scalability and reliability. As the number of users and the amount of data grows, Network Attached Storage is becoming a critical technology and the need for an optimized solution is becoming an important requirement.

Proware delivers the Epica NAS system together with the proNAS management solution, proNAS High-Availability and proBackup client backup solution to provide businesses with the most flexible, scalable, securable and manageable NAS environment. It helps to control the total cost of ownership for data management.

The NAS is a SAS/SATA II NAS system with proNAS 1.1 operating system. It enhances system availability, and manages complex storage environments easily. For improving business productivity and minimizing business risks, the NAS provides volume replication and volume snapshot function. It is also a full featured data protection system supporting RAID levels 0, 1, 5, 6, 10, 50, 60. It supports hot spares, automatic hot rebuild and online capacity expansion within the enclosure.

1.1 Key Features

- Configurable to 19" rack-mountable 2U chassis
- Supports up to Twelve (12) 1" hot-swappable SAS/SATA II hard drives
- Supports Tape/DAT backup/restore (Option)
- Supports RAID levels 0, 1, 5, 6, 10, 50 and 60
- Smart-function LCD panel for ENC status
- Supports hot spare, automatic hot rebuild and online expansion file system
- Allows online capacity expansion within the enclosure
- Two Gigabit Ethernet ports, Support optional 10 Gigabit Ethernet
- Linux-based embedded system (256MB Disk on Module)
- Centralization of Data and Storage Management
- Using Market-Leading Java Technology
- Latest volume snapshot technology
- Apply volume replication to enhance data protection
- Support logical volume over 2TB
- Support iSCSI Target and iSCSI Target trunking
- Support SFTP file transmission
- Support SNMP remote monitor system with hardware status
- Support Ethernet trunking to 8 ports
- Data Backup via backup plan and scheduling
- Enhance system configuration backup

1.2 Technical Specifications

Hardware Platform	Intel Quad Core Xeon 2.0G or above, single / dual Processor
	Cache memory : 2GB DDR2 533/667 ECC REG DIMM up to 12GB
	Two Gigabit Ethernet ports (10 Gigabit Ethernet option)
	Up to Twelve (12)1" hot-swappable SAS/SATA II (3Gb/s, NCQ support) hard drives
	Real time drive activity and status indicators
	Environmental monitoring unit
	Two(2) 600W hot-swap power supplies with PFC
	Expansion PCI slot for H/W upgrade
RAID Controller	LSI SAS 8704EM2 500MHz PowerPC
	RAID level RAID 0, 1, 5, 6, 10, 50 and 60
	Supports 128MB 667 DDRII cache memory
	Supports hot spare and automatic hot rebuild
	Allows online capacity expansion within the enclosure
	Local audible event notification alarm
Storage Management	Volume Management
	Disk usage statistics
	Hot spare capability
	Volume Snapshot
	Volume Replication
Connectivity	SMB, CIFS over TCP/IP
	NFS over UDP/IP
	Cross platform data access
	Novell Netware support
	FTP, HTTP file transfer
	DHCP
	NAT
	Internet gateway
	WINS Server
	Unit acts as a DHCP server
	Unit acts as a master browser
	Share level security
	File level security
	User ID security for NFS
Macintosh Support	AFP over Apple Talk
	AFP over TCP/IP
	Mac zones
General	File Server Independent
	Peer-to-peer operation

	Localized language support
	Supports NIC / trunking / load balance / fail over
	Support UPS management
System Management	Automatic IP address configuration
	Self-contained unit - no extras needed
	Management through Web browser
	Flash upgradeable unit
	Supports Microsoft ADS (2000/2003/2008) / PDC and Unix NIS accounts import
	SNMP / MRTG management and notification
	Fail-free online firmware upgrade
	Unicode support
	Multi-node Management GUI
	CLI management via Telnet or SSH
Data Protection	proNAS High Availabiltiy (option)
	proBackup Client Backup
	proNAS Data and Configuration Backup
	Support Veritas BackupExec Agent
	Support CA ARCserver Agent
	Support Netvault Agent
	Support Acronis True Image backup software
Power Requirements	AC 90V ~ 264V Full range
	10A ~ 5A, 47Hz ~ 63Hz
Physical Dimension	88(H) x 482(W) x 755(D) mm

1.3 RAID Concepts

RAID Fundamentals

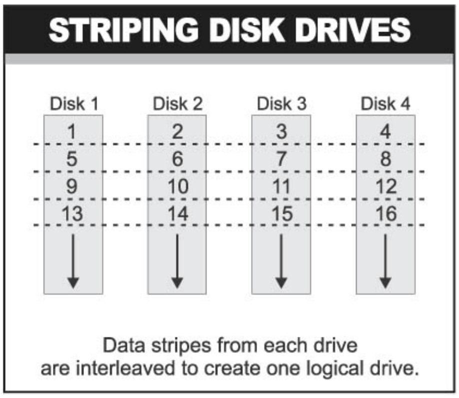
The basic idea of RAID (Redundant Array of Independent Disks) is to combine multiple inexpensive disk drives into an array of disk drives to obtain performance, capacity and reliability that exceeds that of a single large drive. The array of drives appears to the host computer as a single logical drive.

Five types of array architectures, RAID 1 through RAID 5, were originally defined; each provides disk fault-tolerance with different compromises in features and performance. In addition to these five redundant array architectures, it has become popular to refer to a non-redundant array of disk drives as a RAID 0 arrays.

Disk Striping

Fundamental to RAID technology is striping. This is a method of combining multiple drives into one logical storage unit. Striping partitions the storage space of each drive into stripes, which can be as small as one sector (512 bytes) or as large as several megabytes. These stripes are then interleaved in a rotating sequence, so that the combined space is composed alternately of stripes from each drive. The specific type of operating environment determines whether large or small stripes should be used.

Most operating systems today support concurrent disk I/O operations across multiple drives. However, in order to maximize throughput for the disk subsystem, the I/O load must be balanced across all the drives so that each drive can be kept busy as much as possible. In a multiple drive system without striping, the disk I/O load is never perfectly balanced. Some drives will contain data files that are frequently accessed and some drives will rarely be accessed.

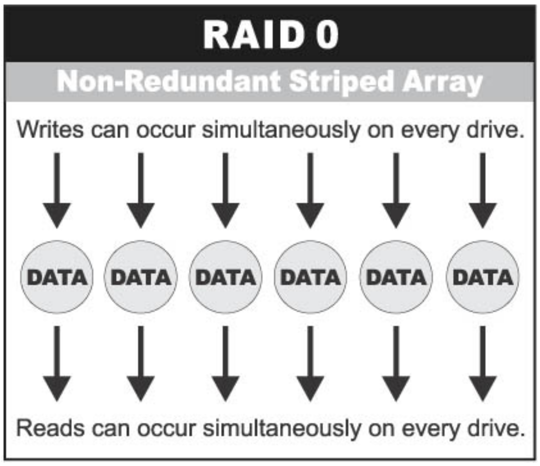


Data stripes from each drive
are interleaved to create one logical drive.

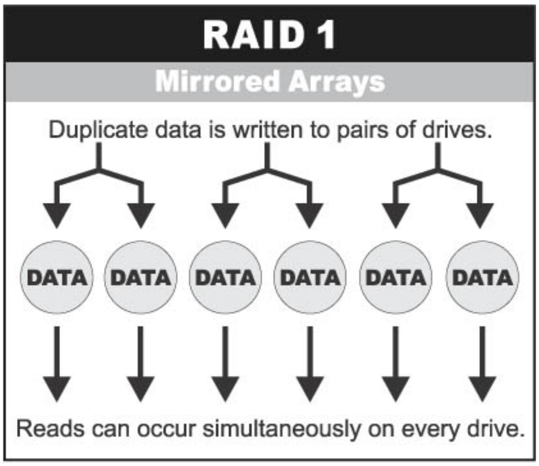
By striping the drives in the array with stripes large enough so that each record falls entirely within one stripe, most records can be evenly distributed across all drives. This keeps all drives in the array busy during heavy load situations. This situation allows all drives to work concurrently on different I/O operations, and thus maximize the number of simultaneous I/O operations that can be performed by the array.

Definition of RAID Levels

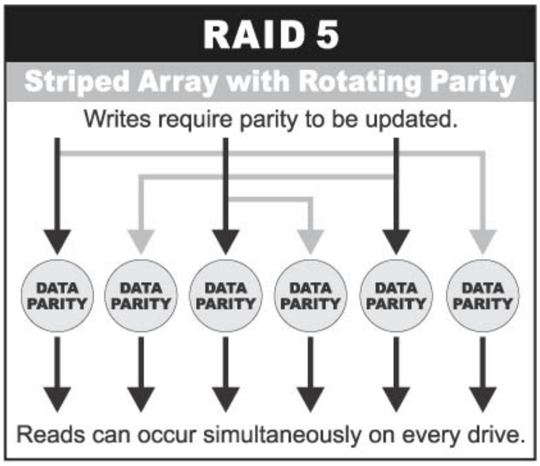
RAID 0 is typically defined as a group of striped disk drives without parity or data redundancy. RAID 0 arrays can be configured with large stripes for multi-user environments or small stripes for single-user systems that access long sequential records. RAID 0 arrays deliver the best data storage efficiency and performance of any array type. The disadvantage is that if one drive in a RAID 0 array fails, the entire array fails.


RAID 0
Non-Redundant Striped Array
Writes can occur simultaneously on every drive.
DATA
DATA
DATA
DATA
DATA
DATA
Reads can occur simultaneously on every drive.

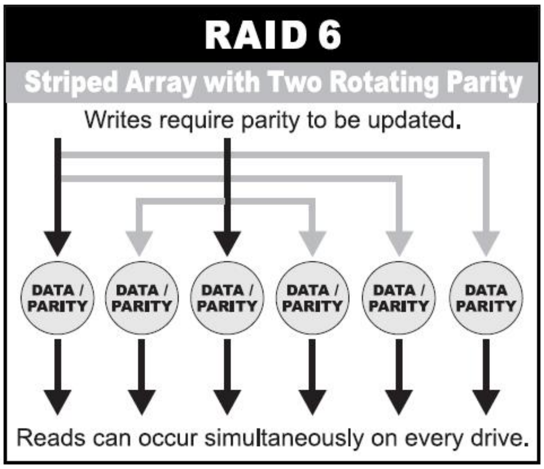
RAID 1, also known as disk mirroring, is simply a pair of disk drives that store duplicate data but appear to the computer as a single drive. Although striping is not used within a single mirrored drive pair, multiple RAID 1 arrays can be striped together to create a single large array consisting of pairs of mirrored drives. All writes must go to both drives of a mirrored pair so that the information on the drives is kept identical. However, each individual drive can perform simultaneous, independent read operations. Mirroring thus doubles the read performance of a single non-mirrored drive and while the write performance is unchanged. RAID 1 delivers the best performance of any redundant array type. In addition, there is less performance degradation during drive failure than in RAID 5 arrays.


RAID 1
Mirrored Arrays
Duplicate data is written to pairs of drives.
DATA
DATA
DATA
DATA
DATA
DATA
Reads can occur simultaneously on every drive.

Under **RAID 5** parity information is distributed across all the drives. Since there is no dedicated parity drive, all drives contain data and read operations can be overlapped on every drive in the array. Write operations will typically access one data drive and one parity drive. However, because different records store their parity on different drives, write operations can usually be overlapped.


RAID 5
Striped Array with Rotating Parity
Writes require parity to be updated.
DATA PARITY
DATA PARITY
DATA PARITY
DATA PARITY
DATA PARITY
DATA PARITY
Reads can occur simultaneously on every drive.

RAID 6 is similar to RAID 5 in that data protection is achieved by writing parity information to the physical drives in the array. With RAID 6, however, ***two*** sets of parity data are used. These two sets are different, and each set occupies a capacity equivalent to that of one of the constituent drives. The main advantage of RAID 6 is High data availability – any two drives can fail without loss of critical data.


RAID 6
Striped Array with Two Rotating Parity
Writes require parity to be updated.
DATA / PARITY
DATA / PARITY
DATA / PARITY
DATA / PARITY
DATA / PARITY
DATA PARITY
Reads can occur simultaneously on every drive.

Dual-level RAID achieves a balance between the increased data availability inherent in RAID 1 and RAID 5 and the increased read performance inherent in disk striping (RAID 0). These arrays are sometimes referred to as RAID 0+1 or RAID 10 and RAID 0+5 or RAID 50.

In summary:

- RAID 0 is the fastest and most efficient array type but offers no fault-tolerance. RAID 0 requires a minimum of two drives.
- RAID 1 is the best choice for performance-critical, fault-tolerant environments. RAID 1 is the only choice for fault-tolerance if no more than two drives are used.
- RAID 5 combines efficient, fault-tolerant data storage with good performance

characteristics. However, write performance and performance during drive failure is slower than with RAID 1. Rebuild operations also require more time than with RAID 1 because parity information is also reconstructed. At least three drives are required for RAID 5 arrays.

- RAID 6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (two-dimensional parity). Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain multiple simultaneous drive failures. It is a perfect solution for mission critical applications.

1.4 Array Definition

1.4.1 Drive Group

A Drive Group is a group of physical drives attached to the RAID controller, and where one or more Virtual Drives (VD) can be created. All Virtual Drives in the Drive Group use all of the physical drives in the Drive Group.

It is not possible to have multiple Disk Groups on the same physical disks. If physical disks of different capacity are grouped together in a Drive Group, then the capacity of the smallest disk will become the effective capacity of all the disks in the Drive Group.

1.4.2 Virtual Drive

A Virtual Drive is seen by the operating system as a single drive or logical device. A Virtual Drive is a storage unit created by the RAID controller from one or more physical drives. If there is an existing Drive Group and there is available Free Space, then a new Virtual Drive can still be created.

Depending on the RAID level used, the Virtual Drive may retain redundant data in case of a drive failure.

Chapter 2 Getting Started

2.1 Packaging, Shipment and Delivery

- ❖ Before removing the subsystem from the shipping carton, you should visually inspect the physical condition of the shipping carton.
- ❖ Unpack the subsystem and verify that the contents of the shipping carton are all there and in good condition.
- ❖ Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.
- ❖ If any damage is found, do not remove the components; contact the dealer where you purchased the subsystem for further instructions.

2.2 Unpacking the NAS System

The package contains the following items:

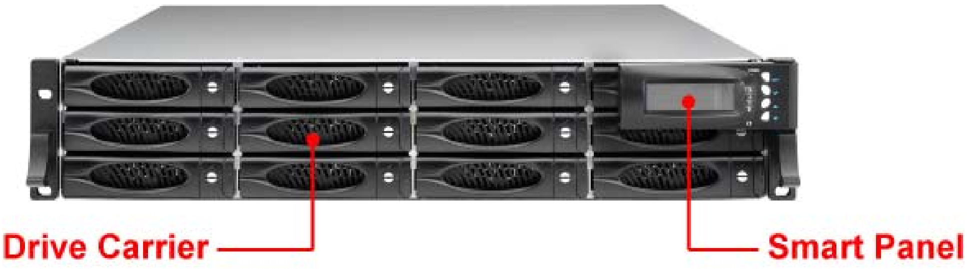
- NAS system unit
- Two (2) power cords
- Two (2) Ethernet LAN cables
- One (1) RS232 null modem cable
- Installation Reference Guide
- Spare screws, etc.

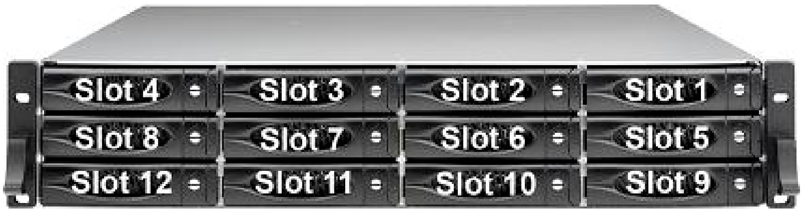
If any of these items are missing or damaged, please contact your dealer or sales representative for assistance.

2.3 Identifying Parts of the NAS System

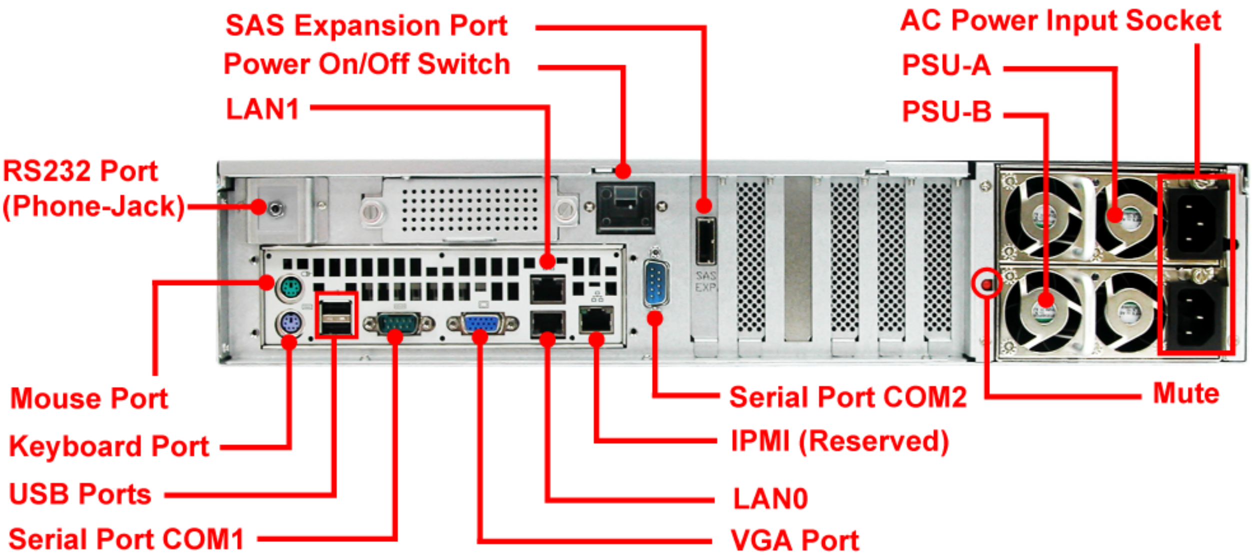
The illustrations below identify the various parts of the subsystem.

2.3.1 Front View





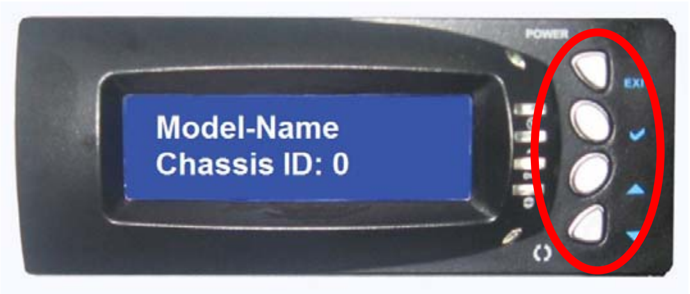
2.3.2 Rear View



1. **Mute** – Use the mute button to stop the power supply buzzer alarm.
2. **RS232 Port (Phone-Jack)** – This is used for upgrading the firmware of JBOD Controller SAS Expander board.
3. **LAN Ports** – The system comes with two 1Gigabit Ethernet ports LAN0 (eth0) and LAN1 (eth1).
4. **SAS Expansion Port** – For connecting to SAS Expansion Chassis.
5. **Serial Ports** – The system has two serial ports COM1 and COM2.
6. **Power On/Off Switch** – Use this switch to power on the system.
7. **PSU-A and B** – Two power supplies are located at the rear of the NAS system.
8. **AC Power Input Socket** – Use this to plug in the power cable connected from power source.
9. **USB ports** – Two USB ports are located at the rear of the system.

2.3.3 LCD Display Panel

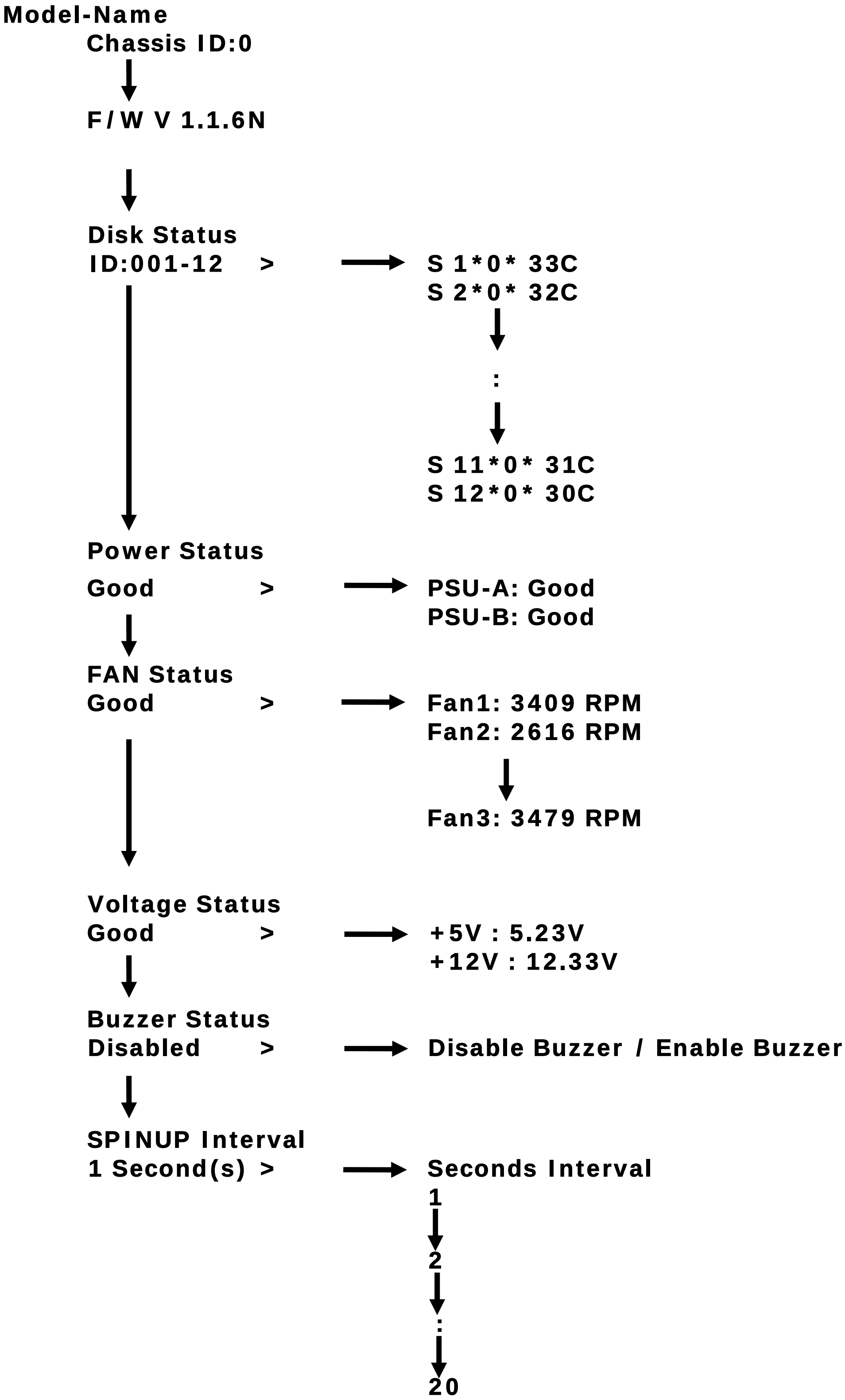
2.3.3.1 LCD Front Panel Function Keys



PARTS	FUNCTION
Up and Down Arrow buttons ▲▼	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu.
Select button ✓	This is used to enter the option you have selected.
Exit button **EXIT**	Press this button to return to the previous menu.

Use the function keys to navigate through the menus in the front panel. The menus will show the JBOD SAS Expander Board firmware version, disk status, fan status, voltage status, and allows you to disable or enable the alarm buzzer.

Menu Diagram



2.4 Drive Carrier Module

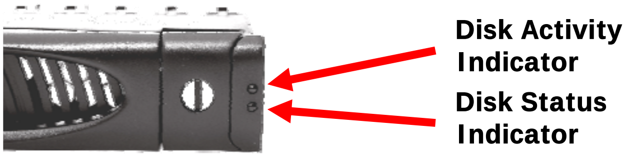
The Drive Carrier Module houses a 3.5 inch hard disk drive. It is designed for maximum airflow and incorporates a carrier locking mechanism to prevent unauthorized access to the HDD.

2.4.1 Disk Drive Status Indicators

Every Drive Carrier has 2 status indicator lights. One indicator light is used for Power On/Error. When this light is **GREEN** the power is on and everything is functioning normally. When the Power On/Error light is **RED**, then an error has occur that requires the user's attention.

The other status indicator light is the hard disk drive access light. When the hard disk drive is being accessed, this light will flash **BLUE**.

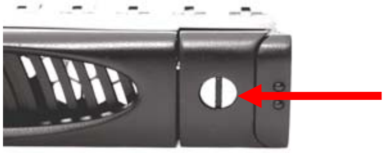
In addition, both indicator lights are viewable within a 170° arc.

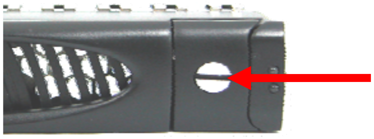


2.4.2 Lock Indicator

Every Drive Carrier is lockable and is fitted with a lock indicator to indicate whether or not the carrier is locked into the chassis or not. Each carrier is also fitted with an ergonomic handle for easy carrier removal.

When the Lock Groove is horizontal, this indicates that the Drive Carrier is locked. When the Lock Groove is vertical, then the Drive Carrier is unlocked. Lock and unlock the Drive Carriers by using a flat-head screw driver.

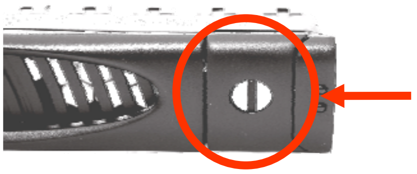




2.5 Installing Hard Drives

This section describes the physical locations of the hard drives supported by the NAS system and give instructions on installing a hard drive. The system supports hot-swapping allowing you to install or replace a hard drive while the NAS system is running.

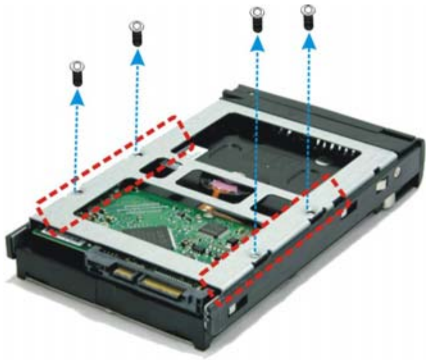
a. To remove a drive tray, make sure it is in unlocked position. Then press the carrier open button. The Drive Carrier handle will flip open.



c. Pull out an empty disk tray. Pull the handle outwards to remove the carrier from the enclosure.

d. Place the hard drive in the disk tray. Make sure the holes of the disk tray align with the holes of the hard drive.

e. Install the mounting screws on the bottom part to secure the drive in the disk tray.



f. Slide the tray into a slot.

g. Close the handle until you hear the latch click into place.

2.6 Preparing the System

1. Attach network cable to the Ethernet port LAN0. Connect the other end to your network switch. You may also connect the other Ethernet LAN port if needed.

2. Connect your VGA monitor to the VGA port.

3. Connect your keyboard and mouse to the keyboard and mouse ports respectively.

2.7 Powering On

1. Plug in the two power cords into the AC Power Input Socket of PSU located at the rear of the NAS system.

NOTE: The NAS system is equipped with redundant, full range power supplies with PFC (power factor correction). The system will automatically select voltage.

2. Open the protective cover of the Power On/Off Switch.
3. Press the Power On/Off Switch to power on the NAS.
4. The Power LED on the front Panel will turn green.
5. Follow the steps in the next chapter to configure a RAID.
6. Follow the steps in the succeeding chapters to configure the NAS system.

Chapter 3 RAID Configuration and Management

Before using the NAS system, a RAID configuration must be created. At least one virtual drive is required to be used in the NAS. You may create more than one Virtual Drive if needed.

3.1 WebBIOS Configuration Utility

The WebBIOS Configuration Utility (CU) enables you to create and manage RAID configurations on LSI SAS controllers. The WebBIOS CU resides in the SAS controller BIOS and operates independently of the operating system.

NOTE: For additional information about the LSI MegaRAID SAS 8704EM2 RAID Configuration and Management, please visit LSI web site:
http://www.lsi.com/DistributionSystem/AssetDocument/files/docs/techdocs/storage_stand_prod/sas/mr_sas_sw_ug.pdf

3.1.1 Starting the WebBIOS Configuration Utility

Perform the following steps to enter the WebBIOS Configuration Utility when you boot the system.

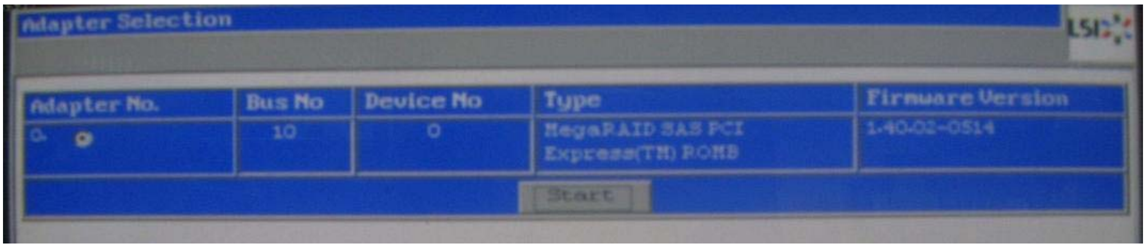
1. When the host computer is booting, hold down the <Ctrl> key and press the <H> key when the following text appears on the screen:

   LSI MegaRAID SAS-MFI BIOS
   Version x.xx.xx
   Copyright© LSI Corporation

   Press <Ctrl><H> for WebBIOS CU

   The Adapter Selection screen appears.

2. Select the SAS MegaRAID Adapter, if not selected.

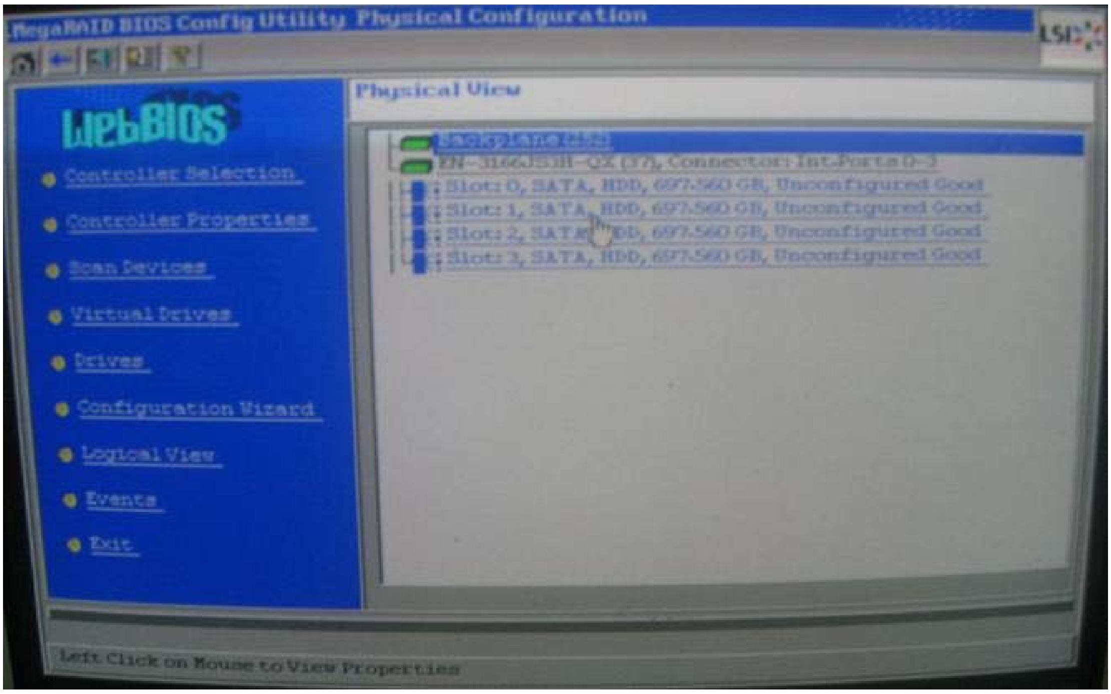


Adapter No.	Bus No	Device No	Type	Firmware Version
0. ●	10	0	MegaRAID SAS PCI Express(TM) ROMB	1-40-02-0514

3. Click **Start** to continue. The main WebBIOS CU screen appears.

3.1.2 WebBIOS CU Main Screen Options

The figure below shows the screen when you start the WebBIOS CU and select an adapter.



Backplane ([illegible])
EN-3166JS3H-QX (37), Connector: Int.Ports 0-3
Slot: 0, SATA, HDD, 697.560 GB, Unconfigured Good
Slot: 1, SATA, HDD, 697.560 GB, Unconfigured Good
Slot: 2, SATA, HDD, 697.560 GB, Unconfigured Good
Slot: 3, SATA, HDD, 697.560 GB, Unconfigured Good

Left Click on Mouse to View Properties

In the lower right panel, the logical view part of the screen displays all of the virtual drives that are configured on this controller. In the upper right panel, the physical view part of the screen displays the drives that are connected to the controller.

To toggle between the physical view and logical view of the storage devices connected to the controller, click **Physical View** or **Logical View** in the menu on the left. When the physical view screen is displayed, the lower right panel displays the drive groups that are configured on this controller.

For drives in an enclosure, the screen displays the drive information in the following format: (Connector): position: slot. The connector information identifies where the chain of enclosures is connected to the RAID controller. The position number identifies the position of the enclosure in the daisy chain.

Directly-attached drives displays in the following format: Slot.

The toolbar at the top of the WebBIOS CU has the following buttons:

Table 3.1.2 WebBIOS CU Toolbar Icons

Icon	Description
🏠	Click this icon to return to the main screen from any other WebBIOS CU screen.
⬅	Click this icon to return to the previous screen that you were viewing.
🚪	Click this icon to exit the WebBIOS CU program.
📁	Click this icon to display the Adapter Selection screen. If the computer system has multiple controllers, you use this screen to view the devices connected to a different controller.
🔈	Click this icon to turn off the sound on the onboard controller alarm.
?	Click this icon to display information about the WebBIOS CU version, browser version, and HTML interface engine.

The WebBIOS CU Main Screen contains the following options:

- **Controller Selection:** Select this to view the Adapter Selection screen, where you can select a different SAS controller. You can then view information about the controller and the devices connected to it, or create a new configuration on the controller.
- **Controller Properties:** Select this to view the properties of the currently selected SAS controller.
- **Scan Devices:** Select this to have the WebBIOS CU re-scan the physical and virtual drives for any changes in the drive status or the physical configuration. The WebBIOS CU displays the results of the scan in the physical and virtual drive descriptions.
- **Virtual Drives:** Select this to view the Virtual Disks screen, where you can change and view virtual drive properties, delete virtual drives, initialize drives, and perform other tasks.
- **Drives:** Select this to view the Drives screen, where you can view drive properties, create hot spares, and perform other tasks.
- **Configuration Wizard:** Select this to start the Configuration Wizard and create a new storage configuration, clear a configuration, or add a configuration.
- **Physical View/Logical View:** Select this to toggle between the Physical View and Logical View screens.
- **Events:** Select this to view system events in the Event Information screen.
- **Exit:** Select this to exit the WebBIOS CU and continue with system boot

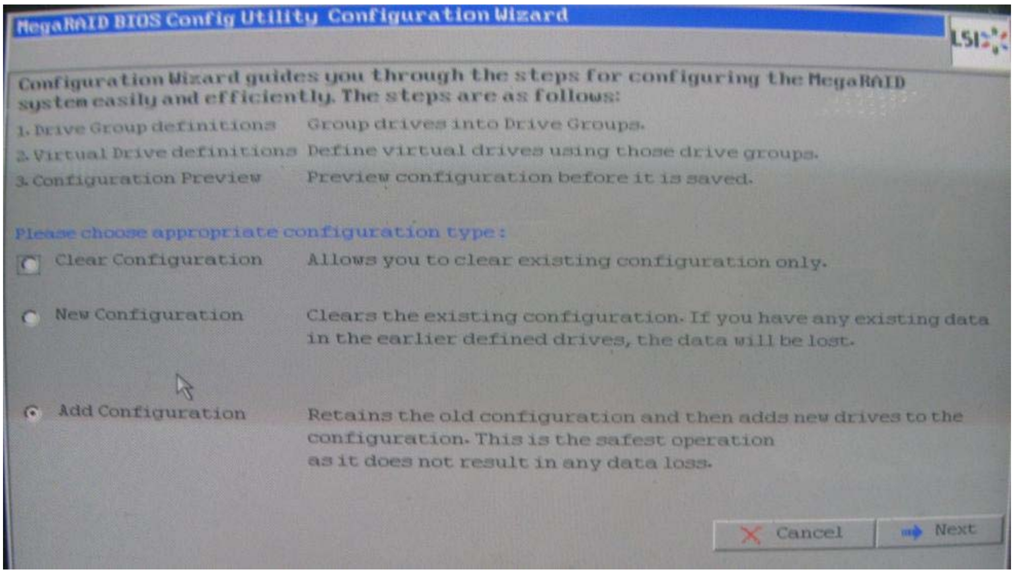
3.2 Configuring RAID Drive Groups and Virtual Drives

NOTE: This section describes the steps to create two RAID Level 5 Virtual Drives to be used in the NAS system.

For additional information about the LSI MegaRAID SAS 8704EM2 RAID Configuration and Management, please visit the LSI web site: http://www.lsi.com/DistributionSystem/AssetDocument/files/docs/techdocs/storage_stand_prod/sas/mr_sas_sw_ug.pdf

To create a RAID configuration:

1. Click **Configuration Wizard** on the WebBIOS main screen. The first Configuration Wizard screen is displayed.



MegaRAID BIOS Config Utility Configuration Wizard

Configuration Wizard guides you through the steps for configuring the MegaRAID system easily and efficiently. The steps are as follows:

1. Drive Group definitions Group drives into Drive Groups.
2. Virtual Drive definitions Define virtual drives using those drive groups.
3. Configuration Preview Preview configuration before it is saved.

Please choose appropriate configuration type:

○ Clear Configuration Allows you to clear existing configuration only.

○ New Configuration Clears the existing configuration. If you have any existing data in the earlier defined drives, the data will be lost.

● Add Configuration Retains the old configuration and then adds new drives to the configuration. This is the safest operation as it does not result in any data loss.

2. Select a configuration option.

WARNING: If you choose the first or second option, all existing data in the configuration will be deleted. Make a backup of any data that you want to keep before you choose an option.

- **Clear Configuration:** Clears the existing configuration.
- **New Configuration:** Clears the existing configuration and lets you create a new configuration.
- **Add Configuration:** Retains the existing storage configuration and adds new drives to it (this does not cause any data loss).

3. To create a new configuration, select **New Configuration**. Click **Next**.

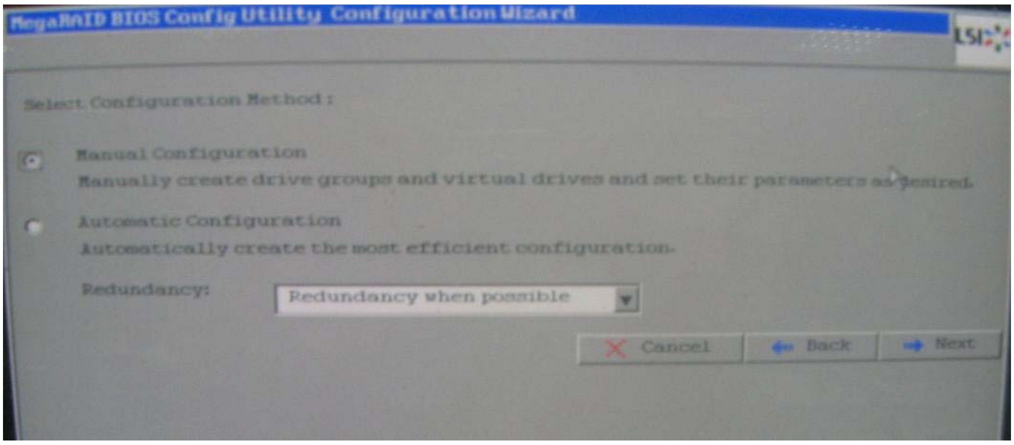
   A dialog box will warn that you will lose data if you select Clear Configuration or New Configuration.

   NOTE: You only select New Configuration the first time you create the drive group and virtual drives. When you add more drives and create new drive groups or virtual drives, you need to select Add Configuration.

4. On the next screen, select **Manual Configuration**.

   Types of Configuration Methods:

   - **Manual Configuration:** Allows you to control all attributes of the new storage configuration.
   - **Automatic Configuration with Redundancy:** Automatically creates an optimal RAID 1, RAID 5, or RAID 6 configuration, providing data redundancy.
   - **Automatic Configuration without Redundancy:** Automatically creates a non-redundant RAID 0 configuration.



MegaRAID BIOS Config Utility Configuration Wizard

Select Configuration Method :

● Manual Configuration
Manually create drive groups and virtual drives and set their parameters as desired.

○ Automatic Configuration
Automatically create the most efficient configuration.

Redundancy: Redundancy when possible

5. Click **Next** to continue.

3.2.1 Using Auto Configuration

If you select one of the Auto Configuration options, either with or without redundancy, the following are the steps to configure RAID:

1. When WebBIOS displays the proposed new configuration, review the information on the screen, and click **Accept** to accept it. (Or click **Back** to go back and change the configuration.)

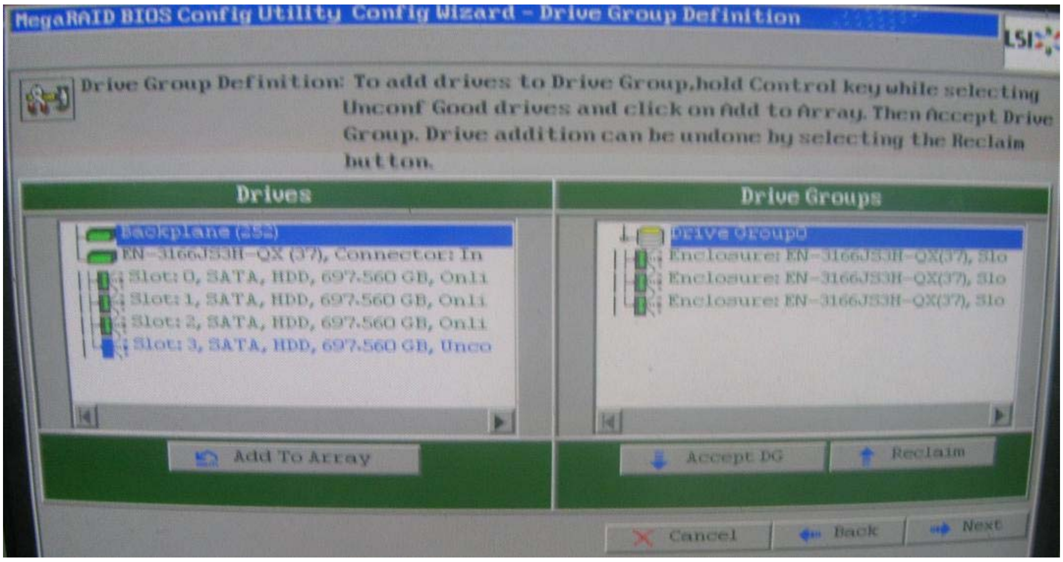
   - **RAID 0:** If you select **Automatic Configuration without Redundancy**, WebBIOS creates a RAID 0 configuration.
   - **RAID 1**: If you select **Automatic Configuration with Redundancy**, and only two drives are available, WebBIOS creates a RAID 1 configuration.
   - **RAID 5**: If you select **Automatic Configuration with Redundancy**, and three or more drives are available, WebBIOS creates a RAID 5 configuration.
   - **RAID 6**: If you select **Automatic Configuration with Redundancy**, and the RAID 6 option is enabled, and three or more drives are available, WebBIOS creates a RAID 6 configuration.
2. Click **Yes** when you are prompted to save the configuration.
3. Click **Yes** when you are prompted to initialize the new virtual drive(s). WebBIOS CU begins a background initialization of the virtual drives.

3.2.2 Using Manual Configuration: Creating RAID 5 Virtual Drives

When you select **Custom Configuration** and click **Next**, the Drive Group Definition screen appears. You use this screen to select drives to create drive groups.

1. Hold <Ctrl> while you select at least three ready drives in the Physical Drives panel on the left.
2. Click **Add to Array** to move the drives to a proposed drive group configuration in the Drive Groups panel on the right.

   If you need to undo the changes, click the **Reclaim** button.



MegaRAID BIOS Config Utility Config Wizard - Drive Group Definition

Drive Group Definition: To add drives to Drive Group,hold Control key while selecting Unconf Good drives and click on Add to Array. Then Accept Drive Group. Drive addition can be undone by selecting the Reclaim button.

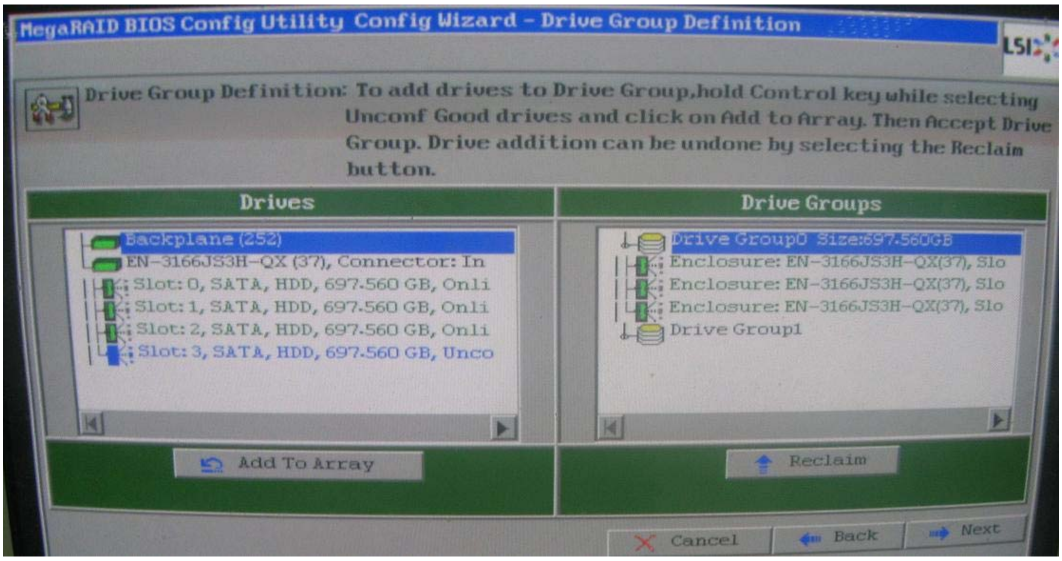
Drives

- Backplane (252)
- EN-3166JS3H-QX (37), Connector: In
- Slot: 0, SATA, HDD, 697.560 GB, Onli
- Slot: 1, SATA, HDD, 697.560 GB, Onli
- Slot: 2, SATA, HDD, 697.560 GB, Onli
- Slot: 3, SATA, HDD, 697.560 GB, Unco

Drive Groups

- Drive Group0
- Enclosure: EN-3166JS3H-QX(37), Slo
- Enclosure: EN-3166JS3H-QX(37), Slo
- Enclosure: EN-3166JS3H-QX(37), Slo

3. When you have finished selecting drives for the drive group, click **Accept DG.**



MegaRAID BIOS Config Utility Config Wizard - Drive Group Definition

Drive Group Definition: To add drives to Drive Group,hold Control key while selecting Unconf Good drives and click on Add to Array. Then Accept Drive Group. Drive addition can be undone by selecting the Reclaim button.

Drives

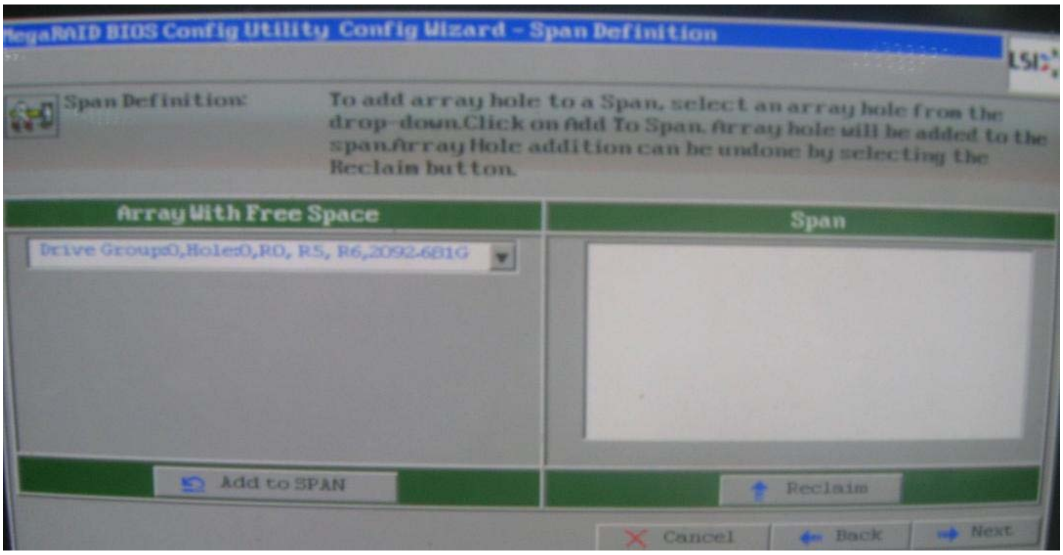
- Backplane (252)
- EN-3166JS3H-QX (37), Connector: In
- Slot: 0, SATA, HDD, 697.560 GB, Onli
- Slot: 1, SATA, HDD, 697.560 GB, Onli
- Slot: 2, SATA, HDD, 697.560 GB, Onli
- Slot: 3, SATA, HDD, 697.560 GB, Unco

Drive Groups

- Drive Group0 Size:697.560GB
- Enclosure: EN-3166JS3H-QX(37), Slo
- Enclosure: EN-3166JS3H-QX(37), Slo
- Enclosure: EN-3166JS3H-QX(37), Slo
- Drive Group1

4. Click **Next**.

5. The Span Definition screen appears. Drive Group 0 is shown in the Array With Free Space list. Click **Add to SPAN**.



MegaRAID BIOS Config Utility Config Wizard - Span Definition

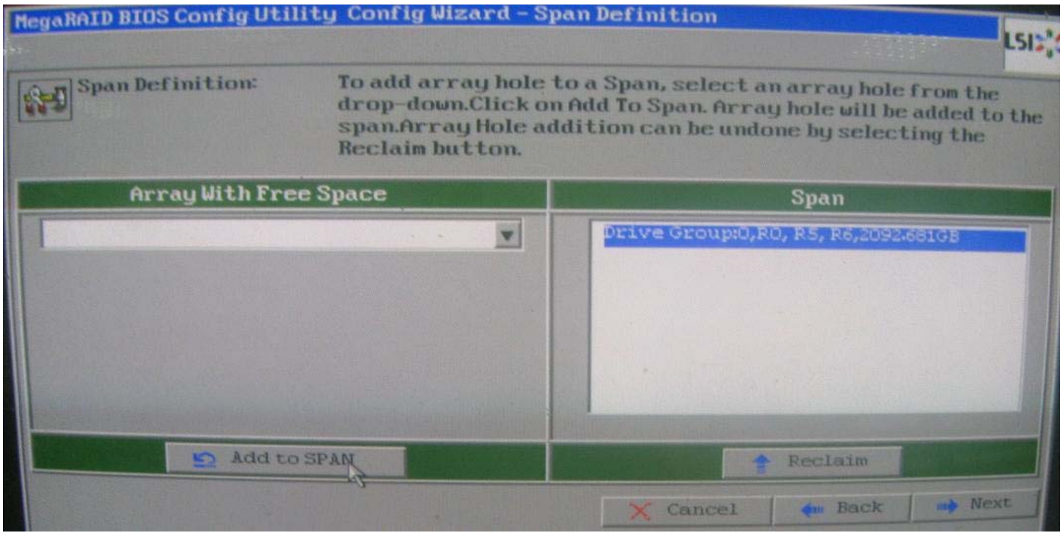
Span Definition:

To add array hole to a Span, select an array hole from the drop-down.Click on Add To Span. Array hole will be added to the span.Array Hole addition can be undone by selecting the Reclaim button.

Array With Free Space: Drive Group:0,Hole:0,R0, R5, R6,2092.681G

Span:

6. Drive Group 0 is listed in the Span panel. Click **Next**.



MegaRAID BIOS Config Utility Config Wizard - Span Definition

Span Definition:

To add array hole to a Span, select an array hole from the drop-down.Click on Add To Span. Array hole will be added to the span.Array Hole addition can be undone by selecting the Reclaim button.

Array With Free Space:

Span: Drive Group:0,R0, R5, R6,2092.681GB

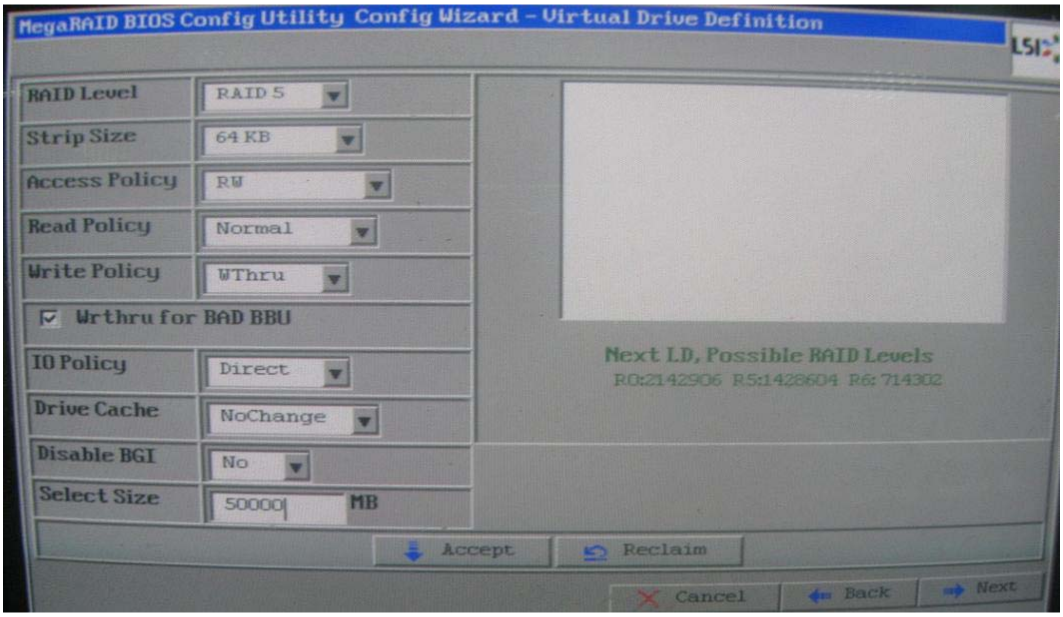
7. The Virtual Drive Definition screen appears. You use this screen to select the RAID level, stripe size, read policy and other attributes for the new virtual drives.

Virtual Drive Parameters and Descriptions

Parameter	Description
RAID Level	The drop-down menu lists the possible RAID levels for the virtual drive.
Stripe Size	The stripe size specifies the length of the data segments that the RAID controller writes across multiple drives, not including parity drives. For example, consider a stripe that contains 64 KB of drive space and has 16 KB of data residing on each drive in the stripe. In this case, the stripe size is 64 KB and the strip size is 16 KB. You can set the stripe size to 8, 16, 32, 64, 128, 256, 512, and 1024 Kbytes. A larger stripe size produces higher read performance. If your computer regularly performs random read requests, choose a smaller stripe size. The default is 64 Kbytes.
Access Policy	Select the type of data access that is allowed for this virtual drive: ➢ *RW*: Allow read/write access. This is the default. ➢ *Read Only*: Allow read-only access. ➢ *Blocked*: Do not allow access.
Read Policy	Specify the read policy for this virtual drive: ➢ *Normal*: This disables the read ahead capability. This is the default. ➢ *Ahead*: This enables read ahead capability, which allows the controller to read sequentially ahead of requested data and to store the additional data in cache memory, anticipating that the data will be needed soon. This speeds up reads for sequential data, but there is little improvement when accessing random data. ➢ *Adaptive*: When Adaptive read ahead is selected, the controller begins using read ahead if the two most recent drive accesses occurred in sequential sectors. If the read requests are random, the controller reverts to *Normal* (no read ahead).
Write Policy	Specify the write policy for this virtual drive: ➢ *WBack*: In Writeback mode the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a transaction. This setting is recommended in Standard mode. ➢ *WThru*: In Writethrough mode the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data in a transaction. This is the default.

	➢ *Bad BBU*: Select this mode if you want the controller to use Writeback mode but the controller has no BBU or the BBU is bad. If you do not choose this option, the controller firmware automatically switches to Writethrough mode if it detects a bad or missing BBU. Caution: LSI allows Writeback mode to be used with or without a battery. LSI recommends that you use **either** a battery to protect the controller cache, or an uninterruptible power supply (UPS) to protect the entire system. If you do not use a battery or a UPS, and there is a power failure, you risk losing the data in the controller cache.
IO Policy	The IO Policy applies to reads on a specific virtual drive. It does not affect the read ahead cache. ➢ *Direct*: In Direct I/O mode, reads are not buffered in cache memory. Data is transferred to the cache and the host concurrently. If the same data block is read again, it comes from cache memory. This is the default. ➢ *Cached*: In Cached I/O mode, all reads are buffered in cache memory.
Drive Cache	Specify the drive cache policy: ➢ *Enable*: Enable the drive cache. ➢ *Disable*: Disable the drive cache. This is the default. ➢ *Unchanged*: Leave the current drive cache policy unchanged.
Disable BGI	Specify the background initialization status: ➢ *No*: Leave background initialization enabled. This means that a new configuration can be initialized in the background while you use WebBIOS to do other configuration tasks. This is the default. ➢ *Yes*: Select *Yes* if you do not want to allow background initializations for configurations on this controller.
Select Size	Specify the size of the virtual drive in megabytes. Normally, this would be the full size for RAID 5 shown in the Configuration panel on the right. You may specify a smaller size if you want to create other virtual drives on the same drive group.

To create Virtual Drive 0, select RAID 5 as RAID Level, and enter the size in Select Size. Click **Accept** then **Next**.



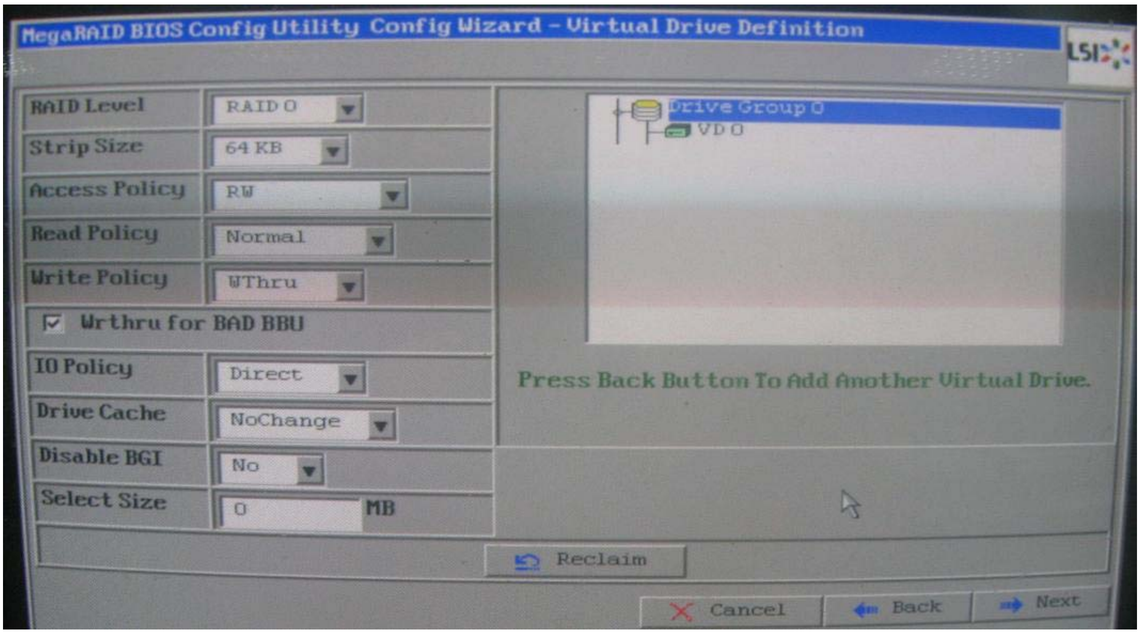
MegaRAID BIOS Config Utility Config Wizard – Virtual Drive Definition

RAID Level: RAID 5
Strip Size: 64 KB
Access Policy: RW
Read Policy: Normal
Write Policy: WThru
☑ Wrthru for BAD BBU
IO Policy: Direct
Drive Cache: NoChange
Disable BGI: No
Select Size: 50000 MB

Next LD, Possible RAID Levels
R0:2142906 R5:1428604 R6: 714302

NOTE: The Virtual Drive can use all of the capacity of the Drive Group. You may create several Virtual Drives depending on your usage and requirement.

8. VD 0 is created. To create the second Virtual Drive, click **Back**. The Span Definition will be displayed. Click **Add to SPAN** and **Next**.



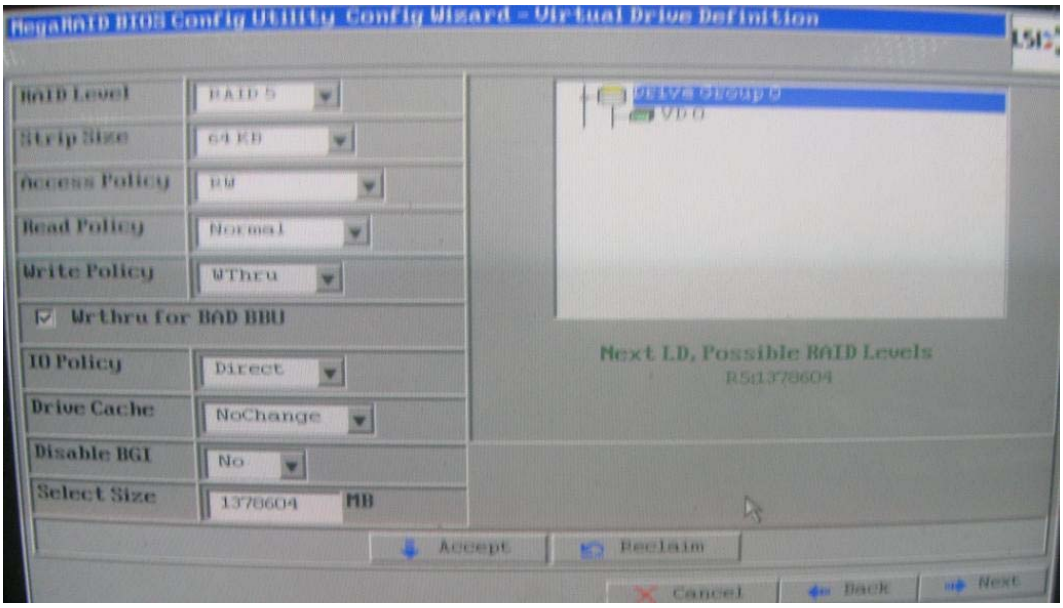
MegaRAID BIOS Config Utility Config Wizard – Virtual Drive Definition

RAID Level: RAID 0
Strip Size: 64 KB
Access Policy: RW
Read Policy: Normal
Write Policy: WThru
☑ Wrthru for BAD BBU
IO Policy: Direct
Drive Cache: NoChange
Disable BGI: No
Select Size: 0 MB

Drive Group 0
VD 0

Press Back Button To Add Another Virtual Drive.

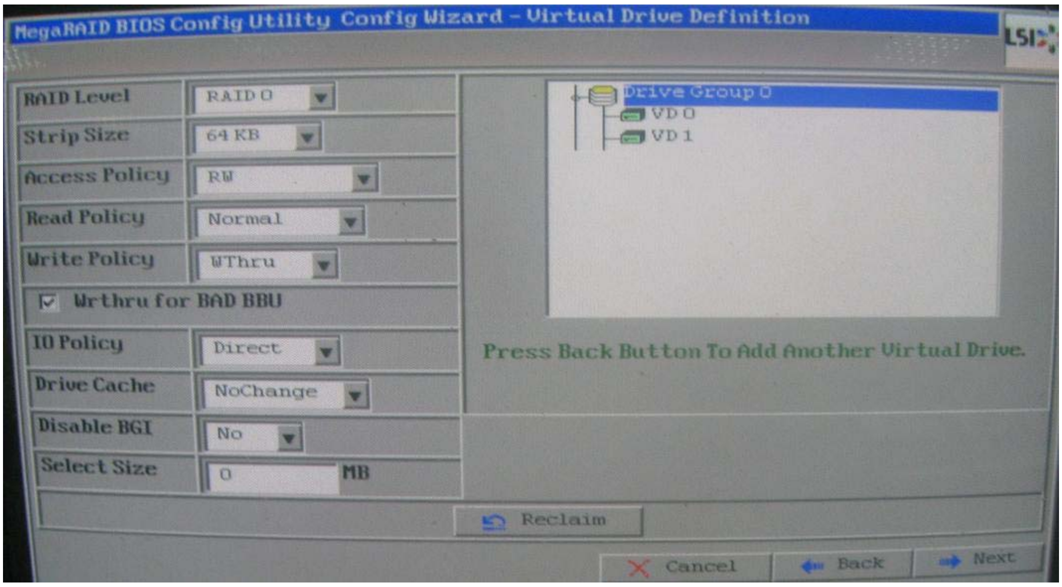
9. The Virtual Disk Definition screen appears. To create Virtual Drive 1, select RAID 5 as RAID Level. The remaining capacity of the Drive Group will be used by Virtual Drive 1. Select **Accept** and click **Next**.


MegaRAID BIOS Config Utility Config Wizard - Virtual Drive Definition
LSI
Drive Group 0
VD 0
Accept
Reclaim
Cancel
Back
Next

RAID Level: RAID 5
Strip Size: 64 KB
Access Policy: RW
Read Policy: Normal
Write Policy: WThru
☑ Wrthru for BAD BBU
IO Policy: Direct
Drive Cache: NoChange
Disable BGI: No
Select Size: 1378604 MB

Next LD, Possible RAID Levels
R5d1378604

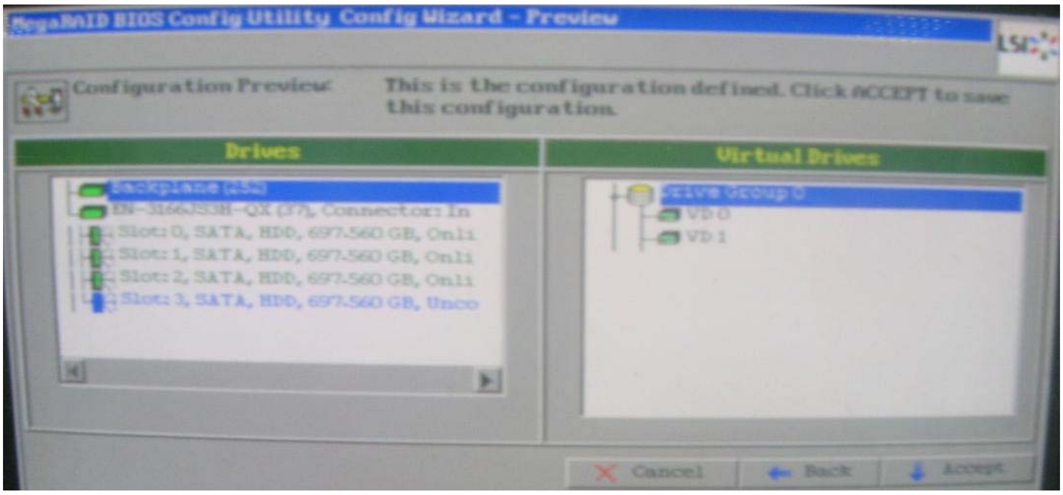
10. Virtual Drive 1 is created. Click **Next**.


MegaRAID BIOS Config Utility Config Wizard - Virtual Drive Definition
LSI
Drive Group 0
VD 0
VD 1
Reclaim
Cancel
Back
Next

RAID Level: RAID 0
Strip Size: 64 KB
Access Policy: RW
Read Policy: Normal
Write Policy: WThru
☑ Wrthru for BAD BBU
IO Policy: Direct
Drive Cache: NoChange
Disable BGI: No
Select Size: 0 MB

Press Back Button To Add Another Virtual Drive.

11. The Configuration Preview screen is shown. Click **Accept** to save the configuration.



MegaRAID BIOS Config Utility Config Wizard - Preview

Configuration Preview: This is the configuration defined. Click ACCEPT to save this configuration.

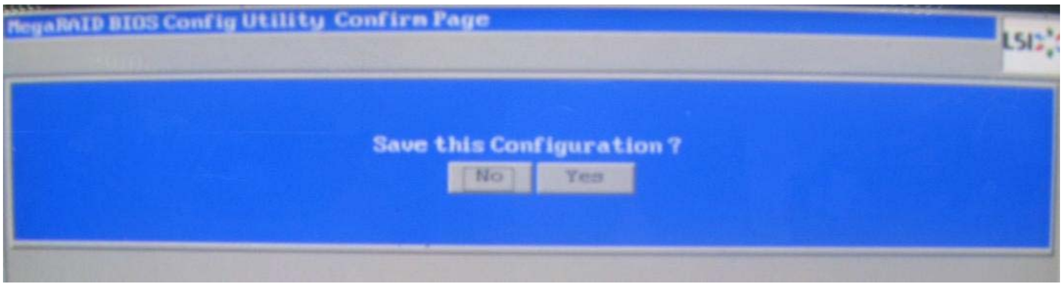
Drives

Backplane (252)
EN-3166JS3H-QX (37), Connector: In
Slot: 0, SATA, HDD, 697.560 GB, Onli
Slot: 1, SATA, HDD, 697.560 GB, Onli
Slot: 2, SATA, HDD, 697.560 GB, Onli
Slot: 3, SATA, HDD, 697.560 GB, Unco

Virtual Drives

Drive Group 0
VD 0
VD 1

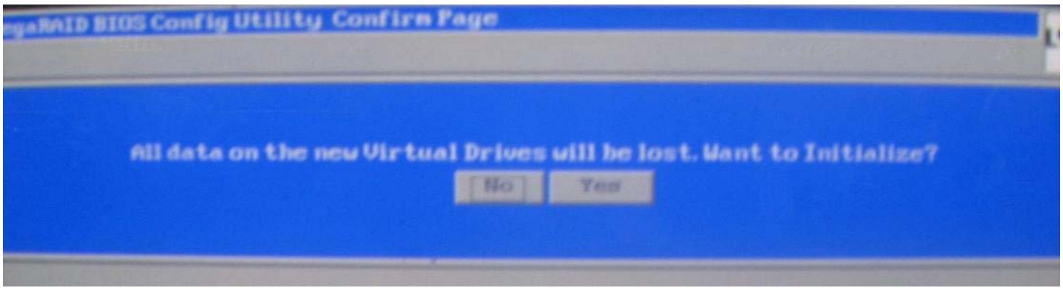
12. A Confirmation Page will be displayed. Select **Yes** to confirm.



MegaRAID BIOS Config Utility Confirm Page

Save this Configuration ?

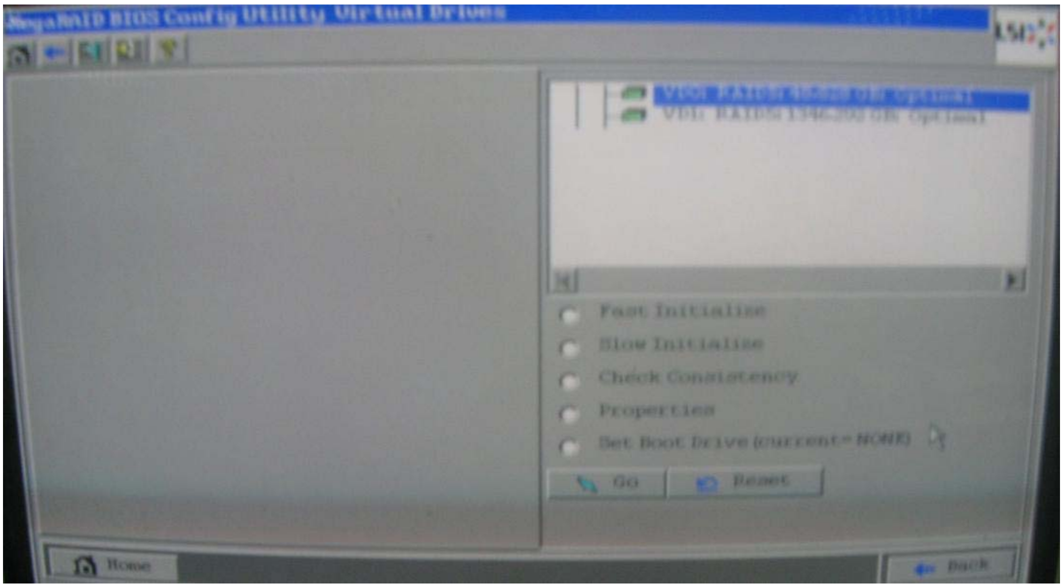
13. Another Confirmation Page is displayed. Select **Yes** to initialize the Virtual Drives.



MegaRAID BIOS Config Utility Confirm Page

All data on the new Virtual Drives will be lost. Want to Initialize?

14. The two Virtual Drives will be initialized in the background. Click **Home** to return to the main screen of WebBIOS CU.

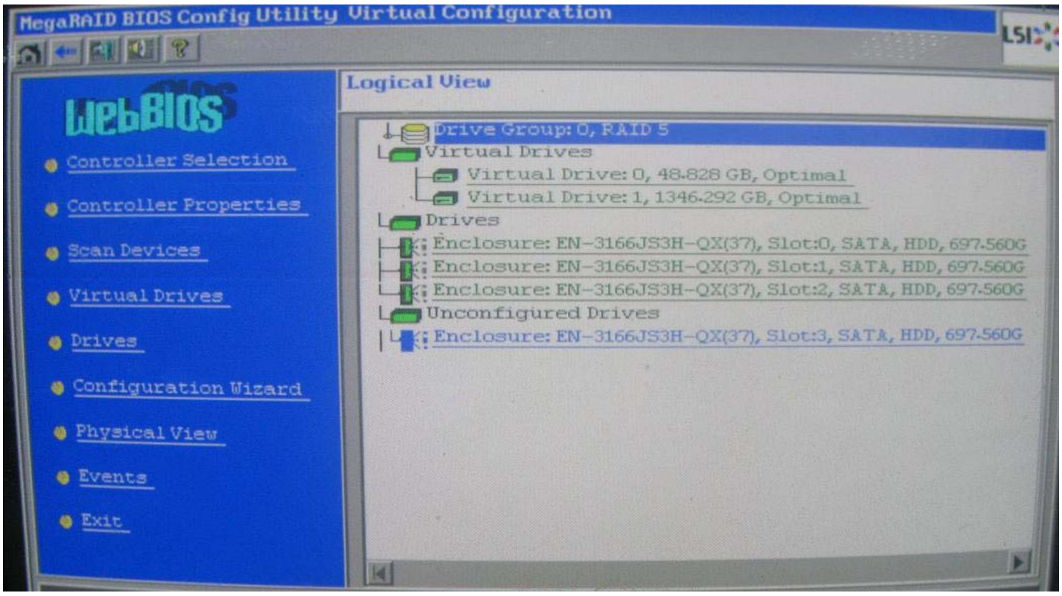

MegaRAID BIOS Config Utility Virtual Drives
LSI
VD1: RAID5: 1346.202 GB, Optimal
○ Fast Initialize
○ Slow Initialize
○ Check Consistency
○ Properties
○ Set Boot Drive (current= NONE)
Go
Reset
Home
Back

3.3 Creating Global Hot Spare

A global hot spare can be used to replace a failed physical disk in any redundant array as long as the capacity of the global hot spare is equal to or larger than the coerced capacity of the failed physical disk.

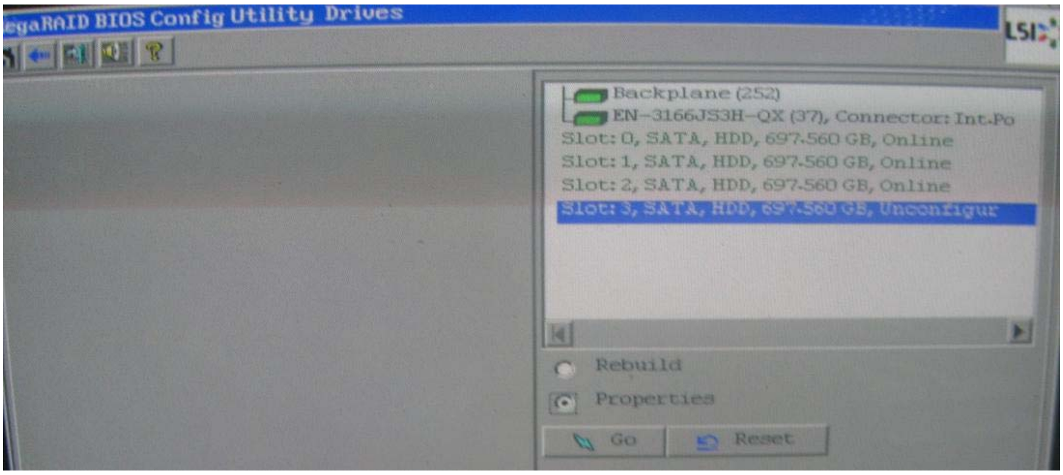
To create a global hot spare:

1. While in WebBIOS CU main screen, select **Drives** option.



```
Drive Group: 0, RAID 5
Virtual Drives
    Virtual Drive: 0, 48.828 GB, Optimal
    Virtual Drive: 1, 1346.292 GB, Optimal
Drives
    Enclosure: EN-3166JS3H-QX(37), Slot:0, SATA, HDD, 697.560G
    Enclosure: EN-3166JS3H-QX(37), Slot:1, SATA, HDD, 697.560G
    Enclosure: EN-3166JS3H-QX(37), Slot:2, SATA, HDD, 697.560G
Unconfigured Drives
    Enclosure: EN-3166JS3H-QX(37), Slot:3, SATA, HDD, 697.560G
```

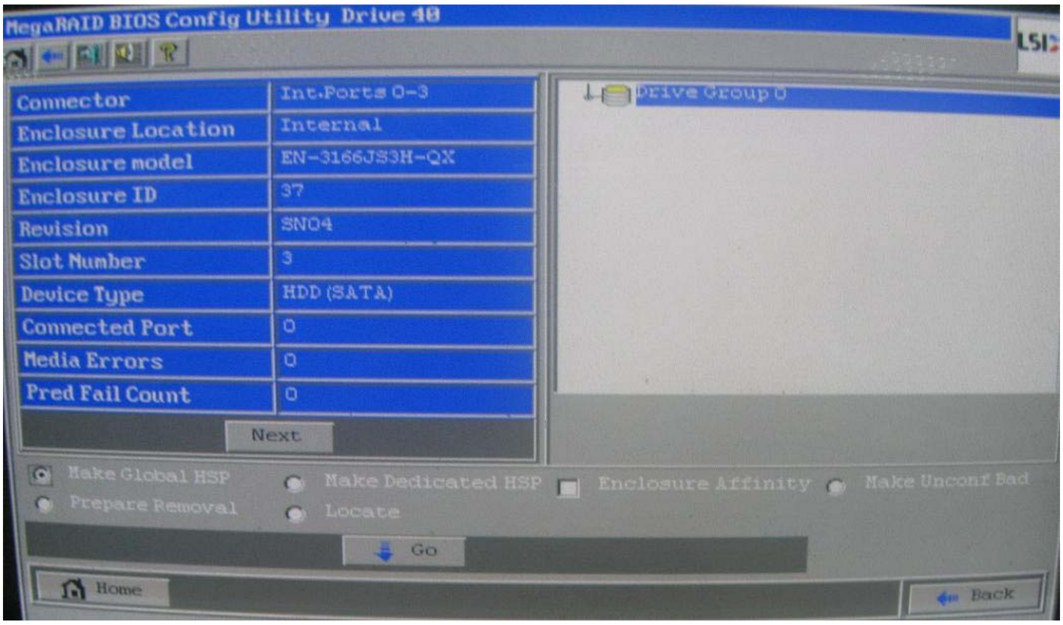
2. Select an un-configured drive and tick **Properties** the click **Go**.



```
Backplane (252)
EN-3166JS3H-QX (37), Connector: Int-Po
Slot: 0, SATA, HDD, 697.560 GB, Online
Slot: 1, SATA, HDD, 697.560 GB, Online
Slot: 2, SATA, HDD, 697.560 GB, Online
Slot: 3, SATA, HDD, 697.560 GB, Unconfigur
```

○ Rebuild
● Properties

3. Choose the **Make Global HSP** option and click **Go**.

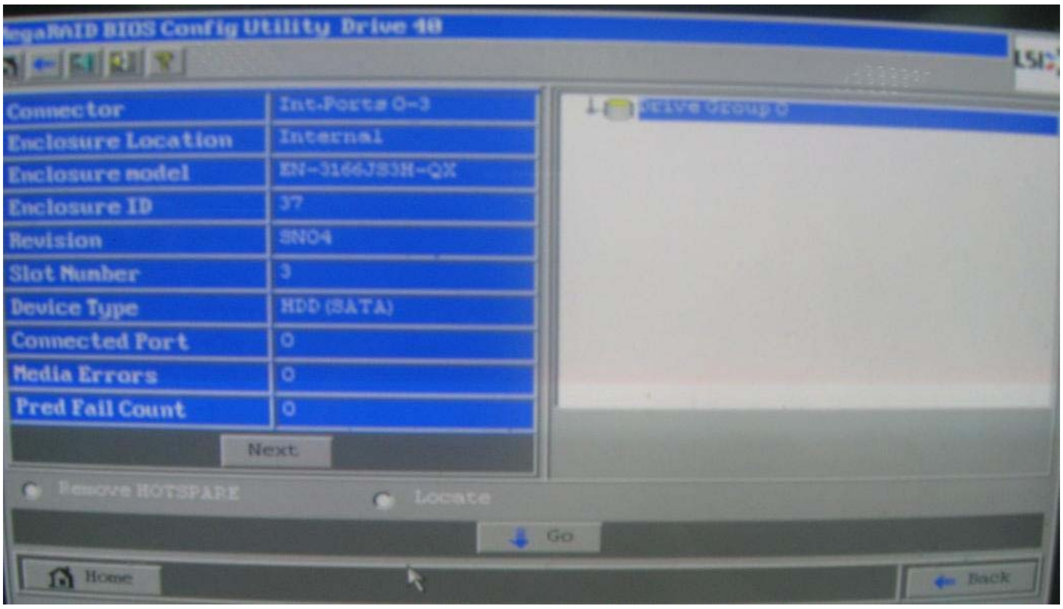


MegaRAID BIOS Config Utility Drive 40

Connector	Int.Ports 0-3
Enclosure Location	Internal
Enclosure model	EN-3166JS3H-QX
Enclosure ID	37
Revision	SN04
Slot Number	3
Device Type	HDD (SATA)
Connected Port	0
Media Errors	0
Pred Fail Count	0

● Make Global HSP ○ Make Dedicated HSP □ Enclosure Affinity ○ Make Unconf Bad
○ Prepare Removal ○ Locate

4. Click **Go**.

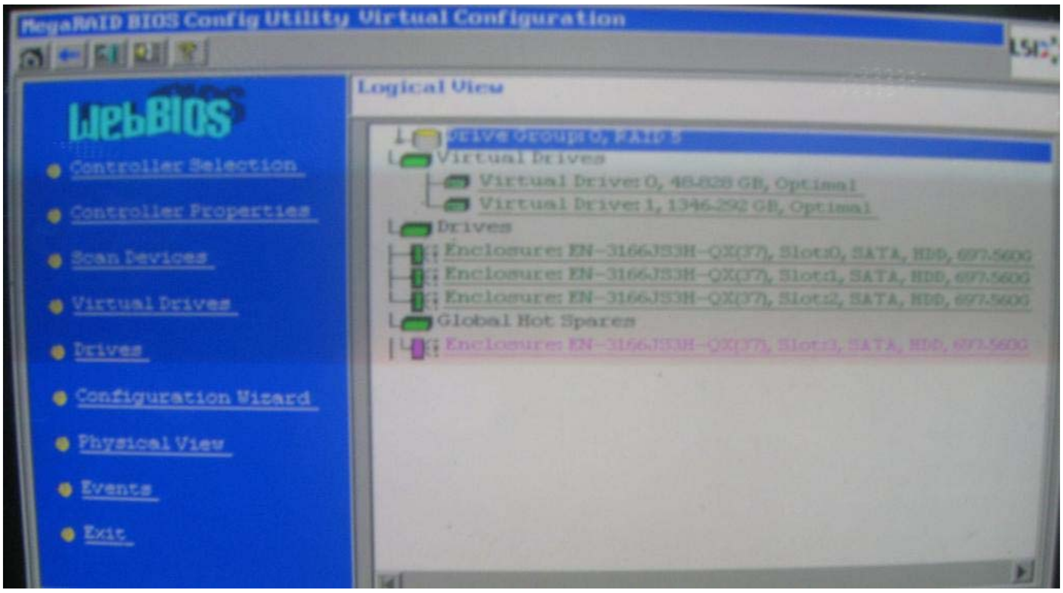


MegaRAID BIOS Config Utility Drive 40

Connector	Int.Ports 0-3
Enclosure Location	Internal
Enclosure model	EN-3166JS3H-QX
Enclosure ID	37
Revision	SN04
Slot Number	3
Device Type	HDD (SATA)
Connected Port	0
Media Errors	0
Pred Fail Count	0

○ Remove HOTSPARE ○ Locate

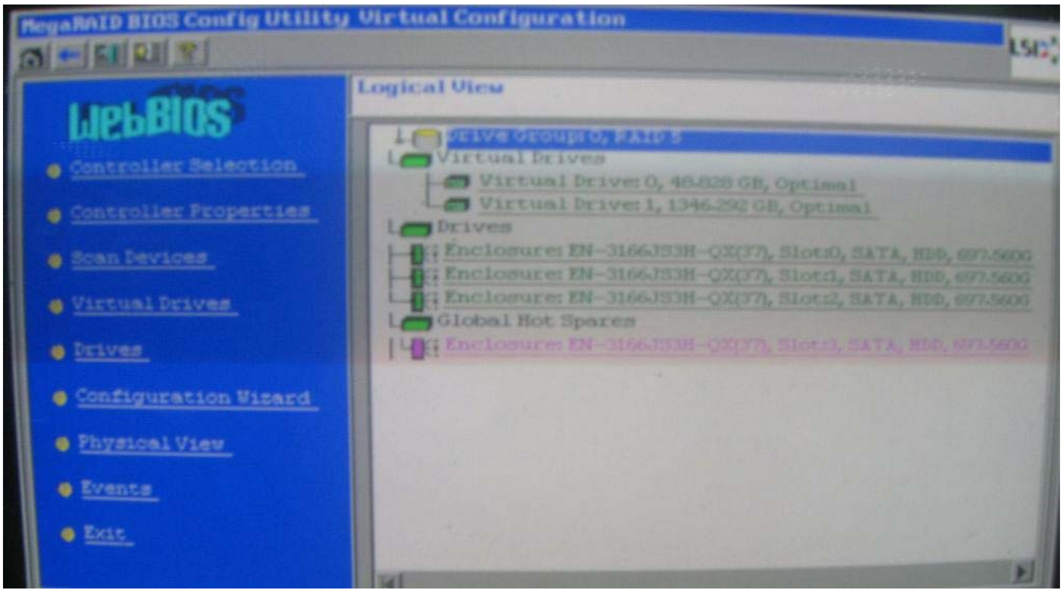
5. The global hot spare drive is created.



```
Drive Group: 0, RAID 5
Virtual Drives
    Virtual Drive: 0, 48.828 GB, Optimal
    Virtual Drive: 1, 1346.292 GB, Optimal
Drives
    Enclosure: EN-3166JS3H-QX(37), Slot:0, SATA, HDD, 697.560G
    Enclosure: EN-3166JS3H-QX(37), Slot:1, SATA, HDD, 697.560G
    Enclosure: EN-3166JS3H-QX(37), Slot:2, SATA, HDD, 697.560G
Global Hot Spares
    Enclosure: EN-3166JS3H-QX(37), Slot:3, SATA, HDD, 697.560G
```

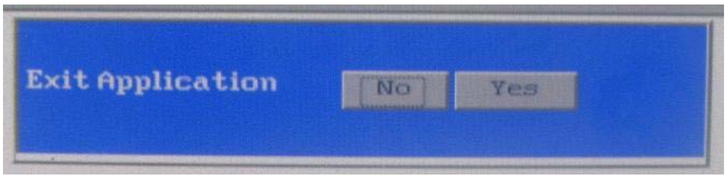
3.4 Restarting the Controller

1. Verify the status of Virtual Drives.



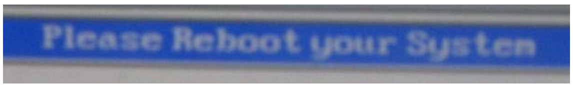
```
Drive Group: 0, RAID 5
Virtual Drives
    Virtual Drive: 0, 48.828 GB, Optimal
    Virtual Drive: 1, 1346.292 GB, Optimal
Drives
    Enclosure: EN-3166JS3H-QX(37), Slot:0, SATA, HDD, 697.560G
    Enclosure: EN-3166JS3H-QX(37), Slot:1, SATA, HDD, 697.560G
    Enclosure: EN-3166JS3H-QX(37), Slot:2, SATA, HDD, 697.560G
Global Hot Spares
    Enclosure: EN-3166JS3H-QX(37), Slot:3, SATA, HDD, 697.560G
```

2. Click **Exit**.
3. A confirmation screen will be displayed. Select **Yes**.



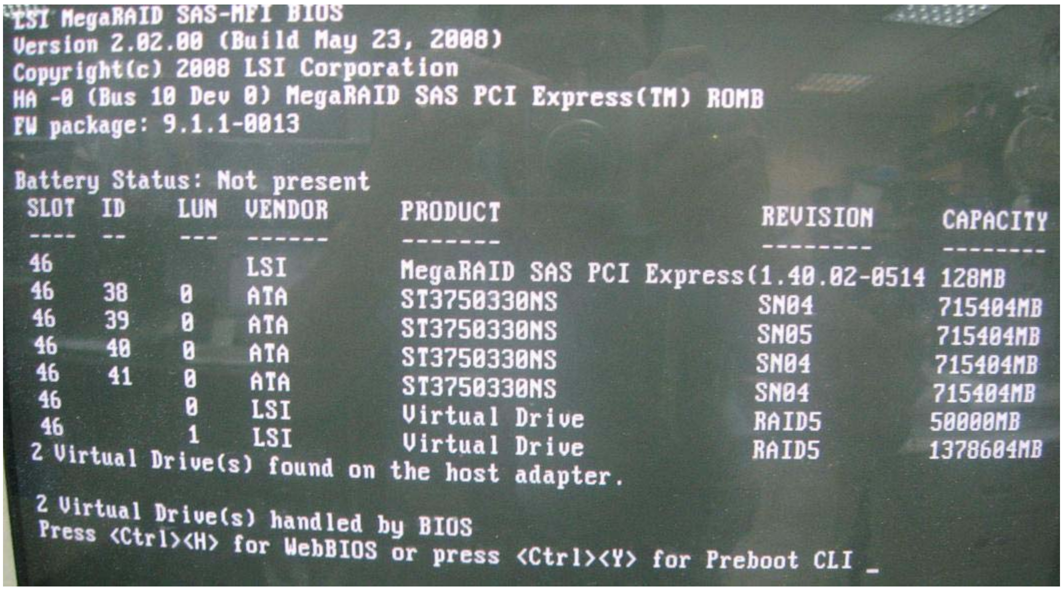
Exit Application

4. A message "Please Reboot your system." Will be displayed. Reboot your system by pressing CTRL+ALT+DEL keys.



Please Reboot your System

5. The system will reboot.



```
LSI MegaRAID SAS-MFI BIOS
Version 2.02.00 (Build May 23, 2008)
Copyright(c) 2008 LSI Corporation
HA -0 (Bus 10 Dev 0) MegaRAID SAS PCI Express(TM) ROMB
FW package: 9.1.1-0013

Battery Status: Not present
 SLOT  ID   LUN  VENDOR     PRODUCT                      REVISION     CAPACITY
 ----  --   ---  ------     -------                      --------     --------
 46               LSI       MegaRAID SAS PCI Express(1.40.02-0514 128MB
 46    38    0    ATA       ST3750330NS                  SN04         715404MB
 46    39    0    ATA       ST3750330NS                  SN05         715404MB
 46    40    0    ATA       ST3750330NS                  SN04         715404MB
 46    41    0    ATA       ST3750330NS                  SN04         715404MB
 46          0    LSI       Virtual Drive                RAID5        50000MB
 46          1    LSI       Virtual Drive                RAID5        1378604MB
2 Virtual Drive(s) found on the host adapter.

2 Virtual Drive(s) handled by BIOS
Press <Ctrl><H> for WebBIOS or press <Ctrl><Y> for Preboot CLI _
```

6. The NAS system will be started. Please refer to Part 2 for the proNAS system configuration.

PART 2 proNAS System

Chapter 4 Introduction

The NAS system comes with “proNAS” NAS management solution and proBackup” client backup solution as well as proNAS HA solution (optional) to provide the enterprises the most flexible, scalable, securable and manageable NAS environment. Administrator can centralize and easily manage the NAS nodes via Internet/Intranet and enhance greater data availability via proNAS.

4.1 proNAS Key Components

- **NAS Device Manager**: Provides configuration of physical hard disks with Hardware RAID Controller.

NOTE: This NAS model does not support NAS Device Manager. Use the WebBIOS CU to configure the RAID controller.

- **proNAS Manager**: Provides several management tools to ease the NAS administration job.
    - Volume Manager: Responsible for volume management. Configuration of volume groups, logical volumes, volume snapshot and volume replication.
    - Account Manager: Local and external account configuration. Import large accounts.
    - Backup Manager: Supports system configuration backup and setup the backup plan for data backup.
    - Share Manager: Share configuration and ACL setting. This also includes Rsync and Duplication functions.
    - System Manager: System configuration and firmware upgrade
    - Network Manager: Configuration of network information and trunking.
    - Log Manager: Contains NAS system logs.
    - Event Manager: Configuration of email notification and system actions when events occur.
- **File Manager**: Provides user logon mode for share owner to perform folder and file management such as share folder access control.
- **proNAS HA**: (optional). Provides function of High Availability (two-node cluster) in Active-Standby mode.
- **proBackup**: Provides web-based GUI backup solution for desktop clients.

Each function of these components is described in the following Chapters.

NOTE: Some pictures and screenshots in the succeeding chapters and sections may be different from the actual machine.

4.2 Installation and Configuration Phases

The installation and configuration of a proNAS system can be divided into five phases.

Phase 1: Set up the Hardware RAID Controller and create Drive Group and Virtual Drive.
Prior to proNAS system configuration, a basic hardware RAID configuration must be setup. Please refer to Chapter 3.

Phase 2: Configure proNAS and its components with proNAS Manager. This is described in details in Chapter 5 proNAS Manager. To configure proNAS, you need to:

- ♦ Join a disk (storage device created in proRAID Manager) to the system default volume group "proNASVG" using Volume Manager. This is described in Chapter 5 Section 5.1.1 to 5.1.2.
- ♦ Configure the network settings via Network Manager. This is described in Chapter 5 Section 5.2.1.
- ♦ Create or import accounts with Account Manager as described in Chapter 5 Section 5.3.
- ♦ Setup the shares using Share Manager and assign account/group permissions. This is described in Chapter 5 Section 5.4.
- ♦ Windows clients can start using the proNAS shares using CIFS protocol. UNIX/Linux clients need to enable NFS protocol (disabled by default).

Phase 3: Perform NAS system maintenance.

- ♦ Maintain system via System Manager, as described in Chapter 5 Section 5.5
- ♦ Check system status using Log Manager and Event Manager. This is described in Chapter 5 Sections 5.7 and 5.8.
- ♦ Backup system configuration and data using Backup Manager. This is described in Chapter 5 Section 5.6.

Phase 4: (Optional) Setup proNAS HA for high-availability environment. Please refer to Chapter 8 for proNAS HA configuration.

Phase 5: Users can store and backup data into proNAS system.

- ♦ Store data into proNAS system using File Manager, as described in Chapter 6.
- ♦ Backup data into proNAS system using proBackup, as described in Chapter 7.

4.3 Setting proNAS IP Address and Connecting to Management GUI

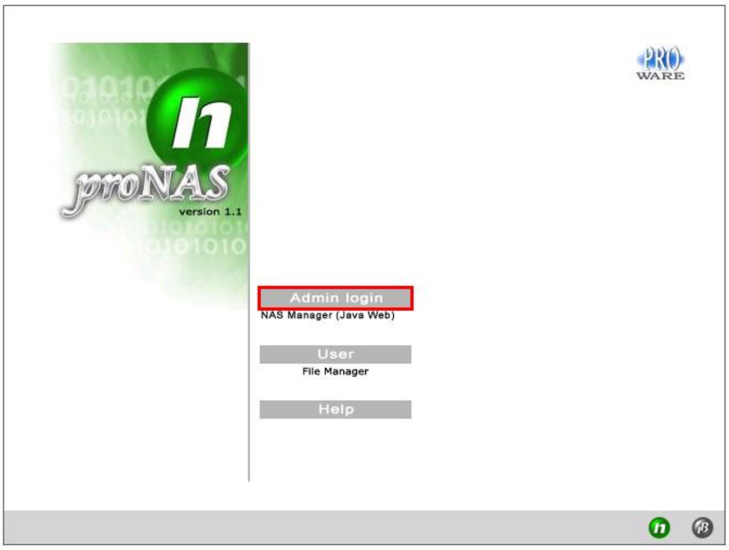
NOTE: Java 2 Runtime Environment (J2RE) 1.4.2 or later must be installed before using the proNAS management interface. (Free download from: http://java.sun.com/j2se/index.jsp)

1. To connect to NAS administration page, change the network settings of your computer to be able to connect to IP address 172.16.0.1 (see table below), or add IP address 172.16.0.5 subnet 255.255.0.0.

Entity	Default Value
LAN IP address	172.16.0.1
Subnet Mask	255.255.0.0
Hostname	proNAS
Username	admin
Password	proware

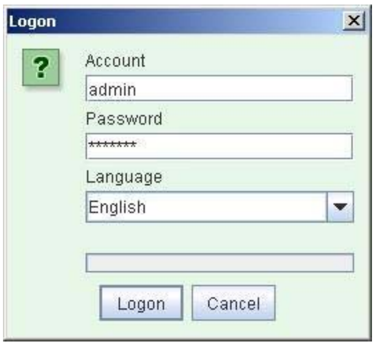
NAS Default Values

2. Open Web browser.
3. Enter the following URL in the address bar: http://172.16.0.1 then press Enter.
4. In the page that opens, click “Admin Login” command button to enter the NAS administration page.



START button on the first proNAS

5. Enter Account as “admin” and password as “proware” and click the Logon command button.



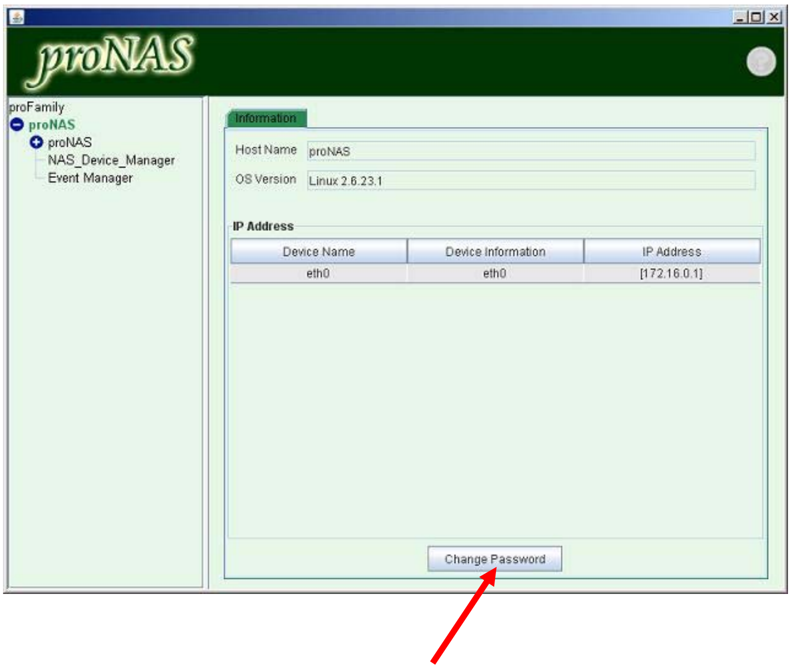
Logon

Account: admin

Password: *******

Language: English

6. The proNAS main screen will be displayed showing proNAS, NAS Device Manager, and Event Manager.



Host Name: proNAS

OS Version: Linux 2.6.23.1

IP Address

Device Name	Device Information	IP Address
eth0	eth0	[172.16.0.1]

“Change Password” option

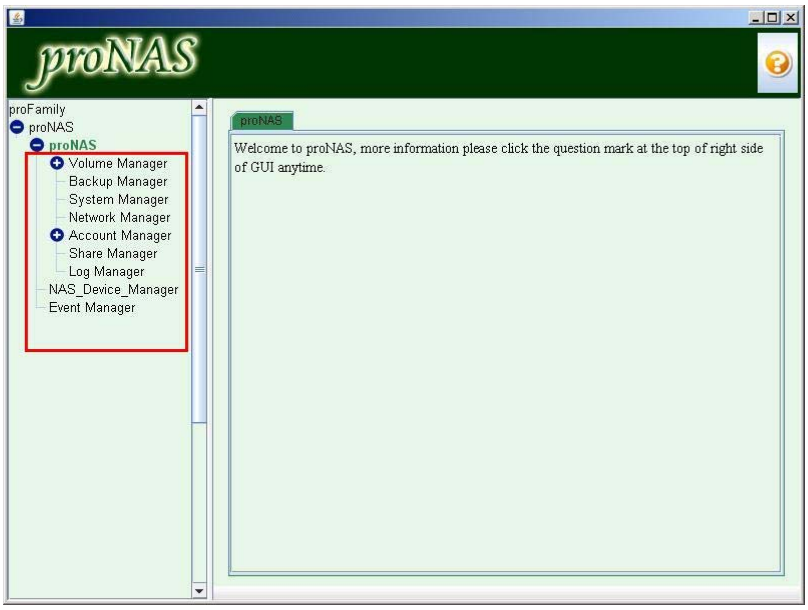
NOTE: For security reason, it is necessary to change the default proNAS admin password. Click the “Change Password” button and enter the new admin password.

Chapter 5 proNAS Manager

proNAS supports Multi-Node Management. If you have several NAS subsystems connected to the intranet, you can see all these systems when you login to the proNAS system. The IP Address section lists the NAS systems connected to the network. proNAS Multi-Node Technology is based on UDP Multi-Casting technology. The proNAS managers are listed below.

The proNAS managers are:

1. Volume Manager
2. Network Manager
3. Account Manager
4. Share Manager
5. System Manager
6. Backup Manager
7. Log Manager
8. Event Manager



Welcome to proNAS, more information please click the question mark at the top of right side of GUI anytime.

5.1 Volume Manager

The Volume Manager is responsible for disk and volume management.

A Volume Group consists of one or more disks that could be individual physical disk(s) or RAID disk(s), which is/are Volume(s) created using proRAID Manager. The default proNAS Volume Group (proNASVG) must be created first by joining at least one "New" or "Non_Initialized" disk to this volume group. The proNASVG holds the NAS system configuration and the default system Logical Volumes, such as home, public, proBackup Device, and proBackup Extended Device, as well as user-defined Logical Volumes. Files and folders reside on these Logical Volumes.

The default proNASVG Volume Group cannot be deleted. When proNASVG is created, the XFS file system is set in each default Logical Volume. XFS file system is also set in all user-defined Logical Volumes. XFS is a high performance journaling file system and provides better recovery time to repair a file system in case of FS damage. The proNAS Volume Group will dynamically allocate some space from its assigned disks, and allocation may fail if no more disk space is available. Therefore, make sure to regularly monitor the available free space of proNAS Volume Group.

The Volume Manager can perform the following function:

- Create a VG (volume group)
- Join New Disks
- Reset a VG (volume group)
- Remove a VG (volume group)
- Create Logical Volume
- Create Snapshot
- Create Replication

5.1.1 Volume Group Management

Volume Group (VG) is created by joining at least one disk, which can be physical disk or RAID disk(s). Logical Volumes are created under the Volume Group.

proNASVG is the system default VG. It must be created first in order to use the NAS system. To create the proNASVG, it is necessary to join at least one “New” or “Non_Initialized” disk into proNASVG. The default proNASVG cannot be deleted or reset.

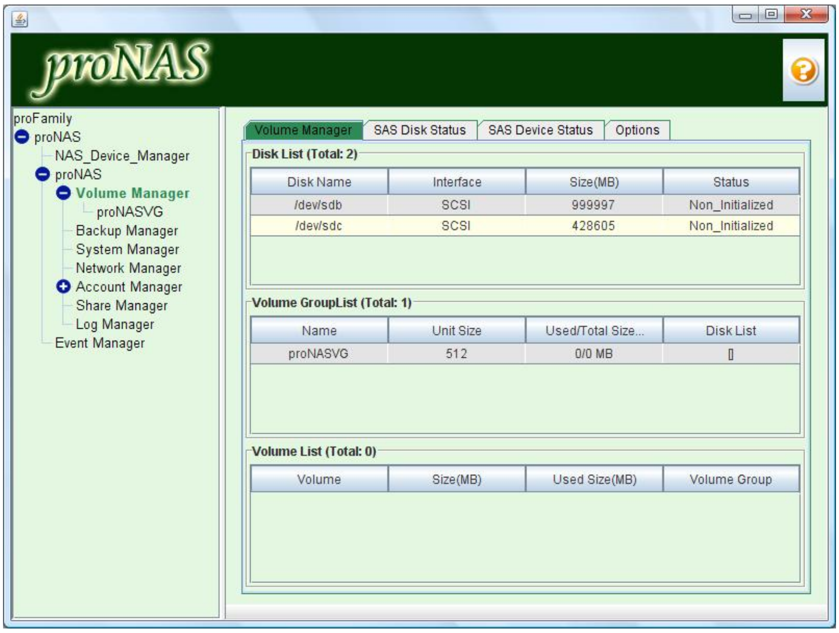
Admin can create other VG by joining other new or “Non_Initialized” disk, create or remove LV in this VG, join any new disk, remove any disk and reset the VG.

NOTE: If the Disk List in Volume Manager does not show any RAID disk (for example: /dev/sda) but a Virtual Drive has been created already, it is necessary to restart the proNAS system. Go to System Manager, select Reboot tab, and click Reboot Now button. Then re-login to NAS administration page.

5.1.1.1 Create the proNASVG Volume Group

To create the proNASVG, perform the following steps:

1. In the proFamily tree, select Volume Manager. Verify that the Disk List shows at least one disk and the Status is “Non_Initialized’. Notice in the Volume Group List that the proNASVG has no Disk List.



Disk List (Total: 2)

Disk Name	Interface	Size(MB)	Status
/dev/sdb	SCSI	999997	Non_Initialized
/dev/sdc	SCSI	428605	Non_Initialized

Volume GroupList (Total: 1)

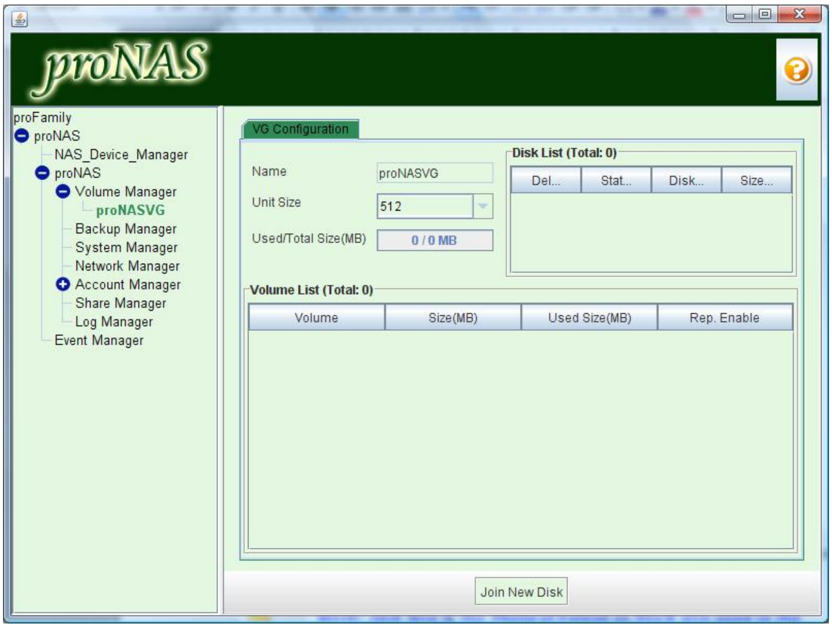
Name	Unit Size	Used/Total Size...	Disk List
proNASVG	512	0/0 MB	[]

Volume List (Total: 0)

Volume	Size(MB)	Used Size(MB)	Volume Group

NOTE: The system default Volume Group “proNASVG” cannot be deleted or reset.

2. Select proNASVG under Volume Manager and click “Join New Disk” button.



Name: proNASVG

Unit Size: 512

Used/Total Size(MB): 0 / 0 MB

Disk List (Total: 0)

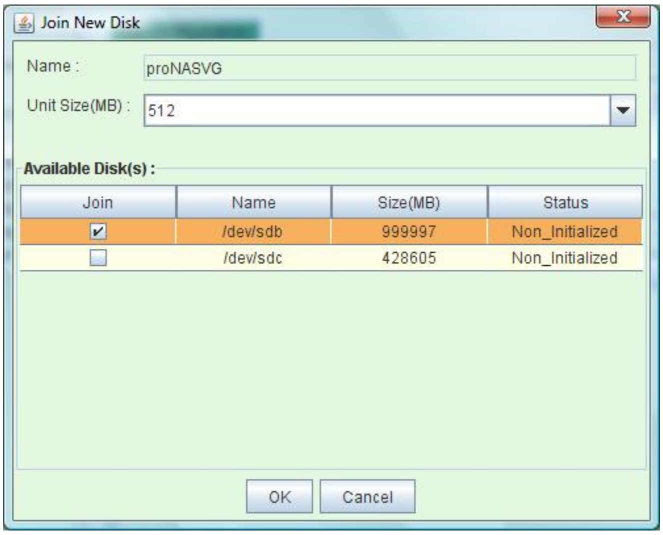
Del...	Stat...	Disk...	Size...

Volume List (Total: 0)

Volume	Size(MB)	Used Size(MB)	Rep. Enable

3. Select the Disk or Disks that will be joined to proNASVG from the list of Available Disk(s). The default Unit Size of proNASVG is 512MB. If needed, the Unit Size can also be changed. Click “OK” when done.

NOTE: Unit Size is the Physical Extent or block size used in the Volume Group.



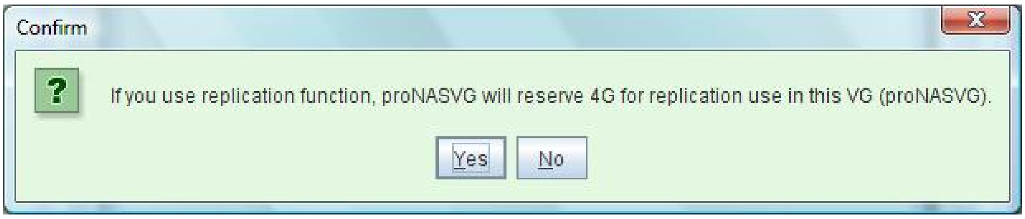
Name : proNASVG

Unit Size(MB) : 512

Available Disk(s) :

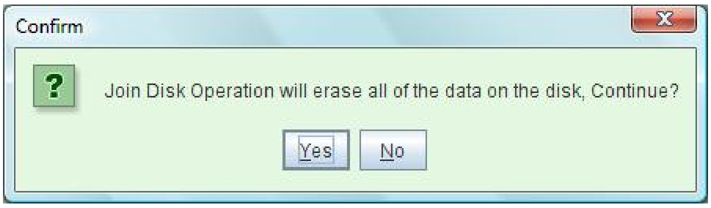
Join	Name	Size(MB)	Status
☑	/dev/sdb	999997	Non_Initialized
□	/dev/sdc	428605	Non_Initialized

4. A confirmation message will appear. Select “Yes” to proceed.



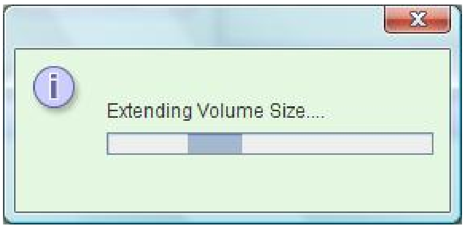
If you use replication function, proNASVG will reserve 4G for replication use in this VG (proNASVG).

5. Another confirmation message will appear. Select “”Yes” to proceed.



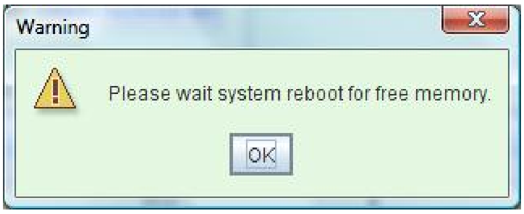
Join Disk Operation will erase all of the data on the disk, Continue?

6. The process of joining disk to the VG will start.



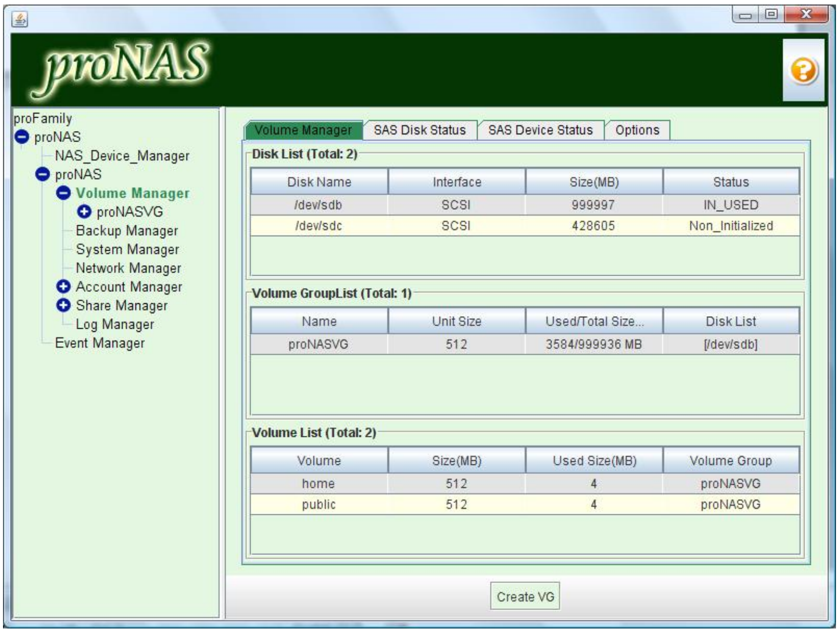
Extending Volume Size....

7. When the process of joining disk to VG is completed, the NAS will reboot to free some used system memory. A warning message will be displayed. Click “OK” to close the message.



Please wait system reboot for free memory.

8. Re-login to proNAS management GUI. The Volume Manager will show the joined disk as “IN_USED” and the Volume List will show the system default Logical Volumes “home” and “public”.



Disk List (Total: 2)

Disk Name	Interface	Size(MB)	Status
/dev/sdb	SCSI	999997	IN_USED
/dev/sdc	SCSI	428605	Non_Initialized

Volume GroupList (Total: 1)

Name	Unit Size	Used/Total Size...	Disk List
proNASVG	512	3584/999936 MB	[/dev/sdb]

Volume List (Total: 2)

Volume	Size(MB)	Used Size(MB)	Volume Group
home	512	4	proNASVG
public	512	4	proNASVG

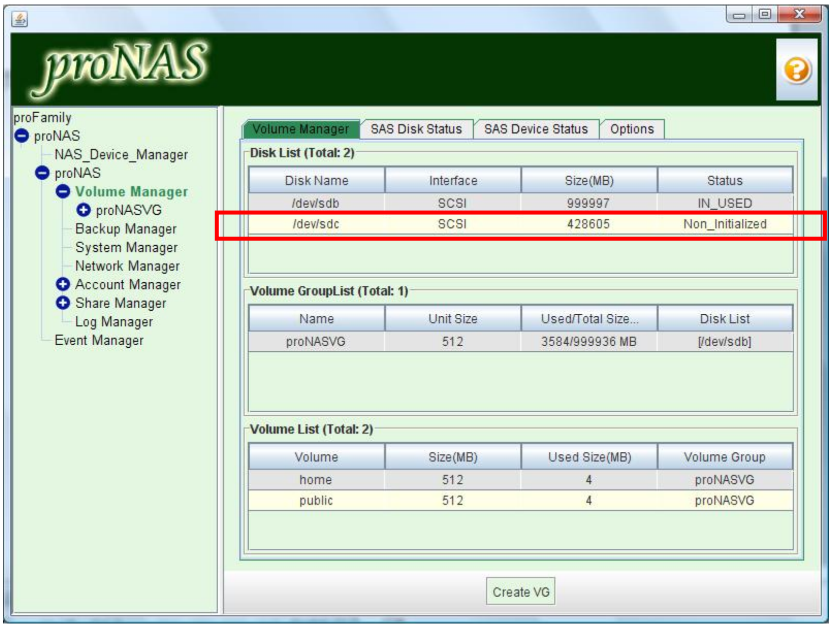
NOTE: The other system default LVs proBackup Device and proBackup Extended Device will only be created and become visible in the Volume List when the proBackup Service is started.

5.1.1.2 Create another Volume Group

To create another VG, verify from Volume Manager Disk List if there is available free or "Non_Initialized" disk. If there is none, a new Virtual Drive (RAID disk) must be created first using WebBIOS CU.

To create another VG, perform the following steps:

1. In Volume Manager, click "Create VG" button.



Disk List (Total: 2)

Disk Name	Interface	Size(MB)	Status
/dev/sdb	SCSI	999997	IN_USED
/dev/sdc	SCSI	428605	Non_Initialized

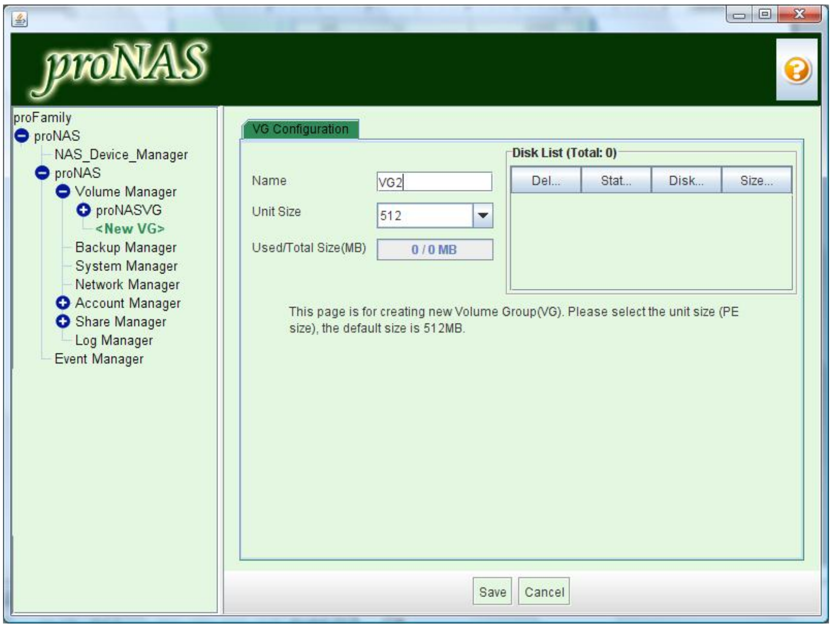
Volume GroupList (Total: 1)

Name	Unit Size	Used/Total Size...	Disk List
proNASVG	512	3584/999936 MB	[/dev/sdb]

Volume List (Total: 2)

Volume	Size(MB)	Used Size(MB)	Volume Group
home	512	4	proNASVG
public	512	4	proNASVG

2. Enter the Volume Group Name. Click "Save" when done.



Name VG2

Unit Size 512

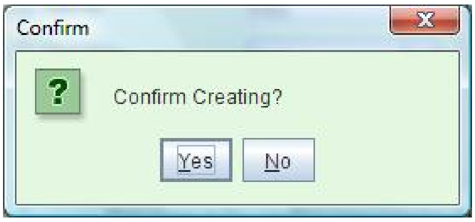
Used/Total Size(MB) 0 / 0 MB

Disk List (Total: 0)

Del...	Stat...	Disk...	Size...

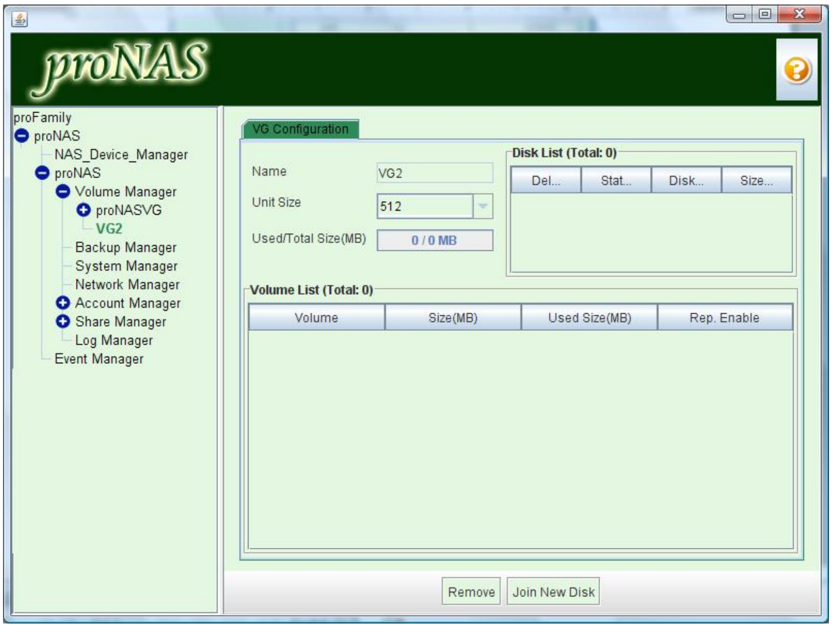
This page is for creating new Volume Group(VG). Please select the unit size (PE size), the default size is 512MB.

3. A confirmation message will appear. Select “Yes” to proceed.



Confirm Creating?

4. Click “Join New Disk” to continue with creating the new Volume Group.



Name: VG2

Unit Size: 512

Used/Total Size(MB): 0 / 0 MB

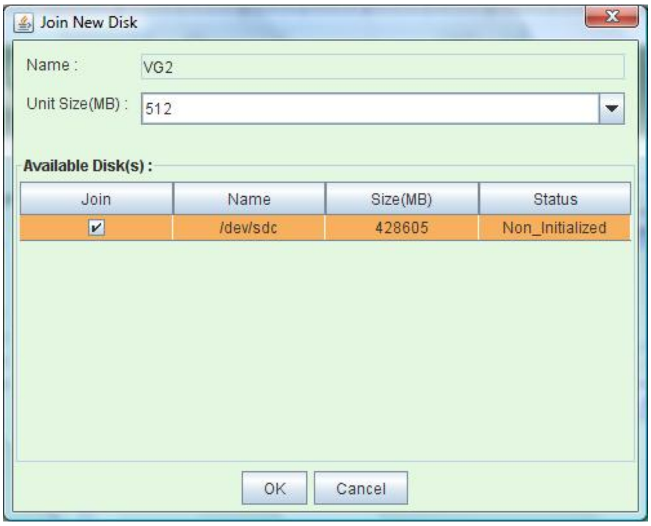
Disk List (Total: 0)

Del...	Stat...	Disk...	Size...

Volume List (Total: 0)

Volume	Size(MB)	Used Size(MB)	Rep. Enable

5. Check the disk(s) to be joined to the VG. Click “OK” when done.



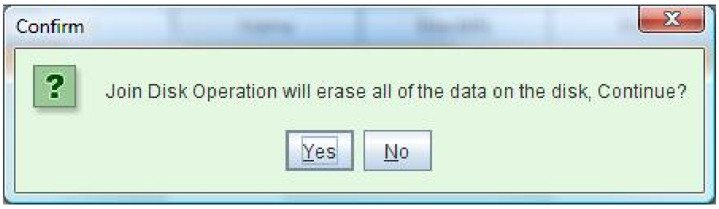
Name : VG2

Unit Size(MB) : 512

Available Disk(s) :

Join	Name	Size(MB)	Status
☑	/dev/sdc	428605	Non_Initialized

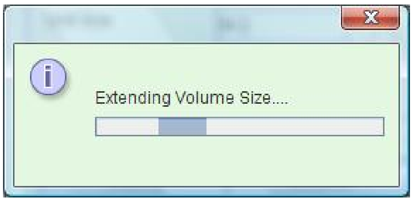
6. A confirmation message will appear. Select “Yes” to proceed.



Confirm

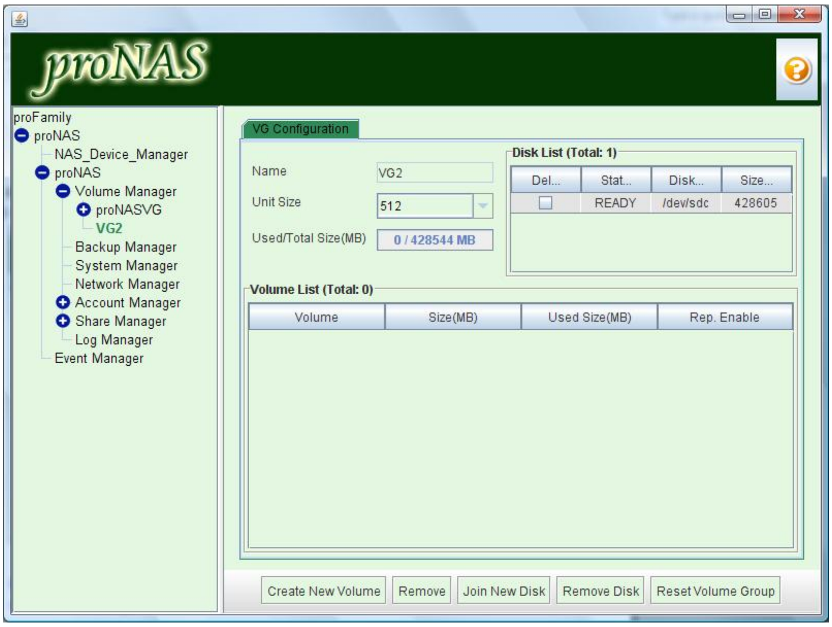
Join Disk Operation will erase all of the data on the disk, Continue?

7. A process window will appear.



Extending Volume Size....

8. When the process of joining disk to the new VG is completed, the newly created VG will be shown.



Name VG2

Unit Size 512

Used/Total Size(MB) 0 / 428544 MB

Disk List (Total: 1)

Del...	Stat...	Disk...	Size...
☐	READY	/dev/sdc	428605

Volume List (Total: 0)

Volume	Size(MB)	Used Size(MB)	Rep. Enable

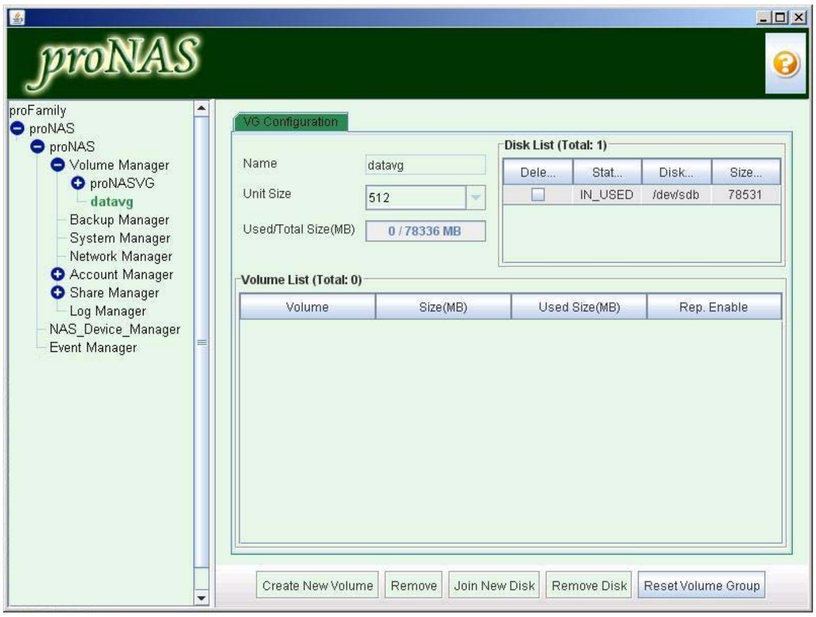
NOTE: The new VG has no default Logical Volumes. Admin can create new Logical Volumes.

NOTE: The NAS supports up to 5 Volume Groups. Volume Group is the highest level abstraction used within the NAS system. It gathers together a collection of Physical Volumes (consisting of at least one disk device, such as /dev/sda) and Logical Volumes into one administrative unit.

5.1.1.3 Reset and Remove Volume Group

If you choose to reset the Volume Group, all the data will be erased. Use the "Reset Volume Group" function only when necessary, and when the data from the VG have been backed up or you do not want to keep the data.

1. Select "Reset Volume Group" button.



Name: datavg
Unit Size: 512
Used/Total Size(MB): 0 / 78336 MB

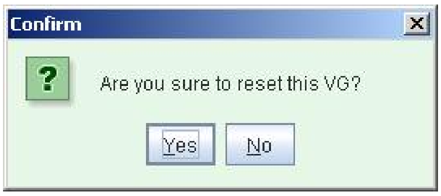
Disk List (Total: 1)

Dele...	Stat...	Disk...	Size...
□	IN_USED	/dev/sdb	78531

Volume List (Total: 0)

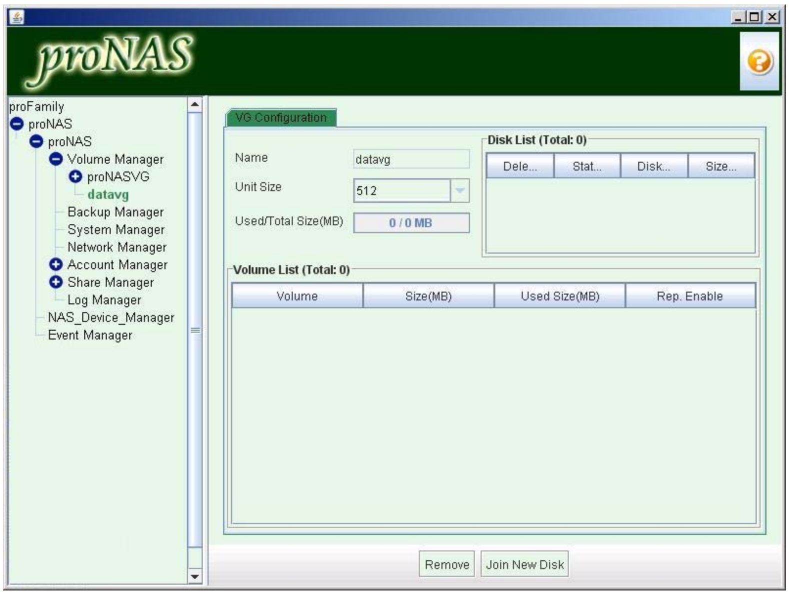
Volume	Size(MB)	Used Size(MB)	Rep. Enable

2. Select "Yes" to confirm.



Are you sure to reset this VG?

3. Click "Remove".



Name: datavg
Unit Size: 512
Used/Total Size(MB): 0 / 0 MB

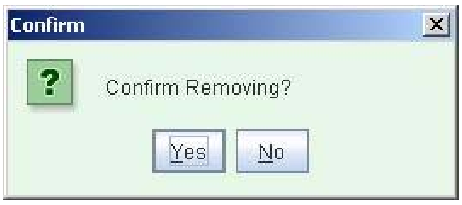
Disk List (Total: 0)

Dele...	Stat...	Disk...	Size...

Volume List (Total: 0)

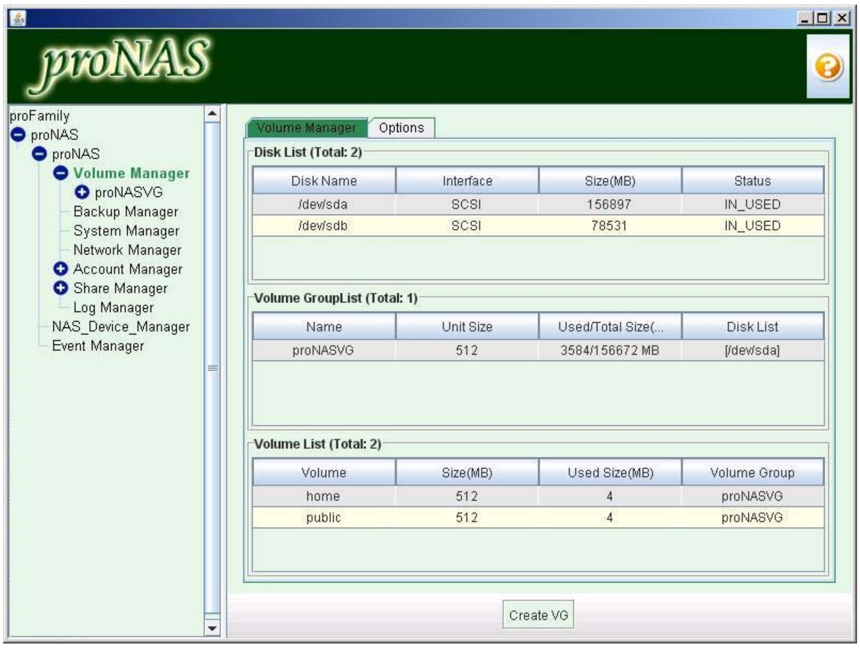
Volume	Size(MB)	Used Size(MB)	Rep. Enable

4. Select “Yes” from the confirmation message.



Confirm Removing?

5. Verify from Volume Group List in Volume Manager that the VG has been removed.



Disk List (Total: 2)

Disk Name	Interface	Size(MB)	Status
/dev/sda	SCSI	156897	IN_USED
/dev/sdb	SCSI	78531	IN_USED

Volume GroupList (Total: 1)

Name	Unit Size	Used/Total Size(...	Disk List
proNASVG	512	3584/156672 MB	[/dev/sda]

Volume List (Total: 2)

Volume	Size(MB)	Used Size(MB)	Volume Group
home	512	4	proNASVG
public	512	4	proNASVG

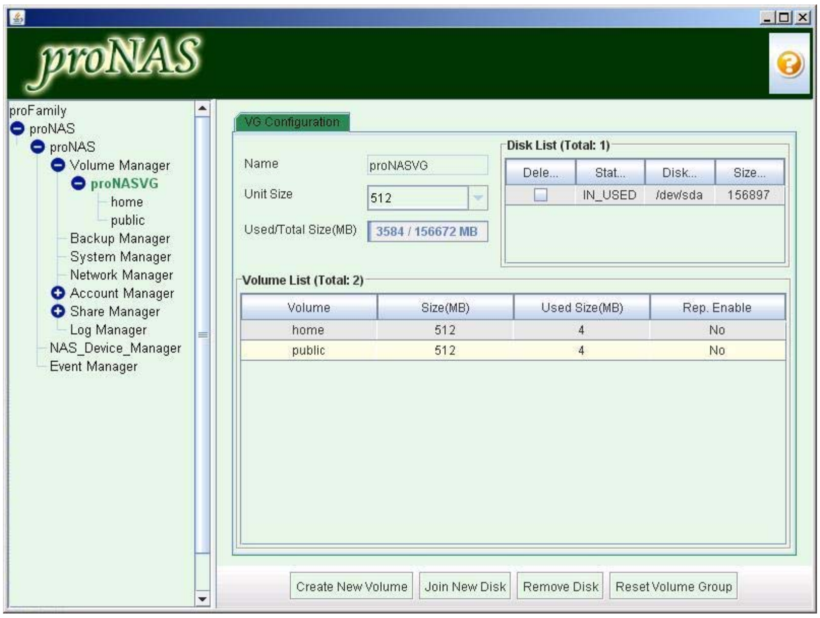
NOTE: The system default Volume Group “proNASVG” cannot be deleted or reset. Only custom created VG can be reset.

5.1.2 Logical Volume Configuration

5.1.2.1 Create new Logical Volume

To create a new Logical Volume, follow these steps:

1. Double-click on a VG name. Click “Create New Volume” button.



Name: proNASVG

Unit Size: 512

Used/Total Size(MB): 3584 / 156672 MB

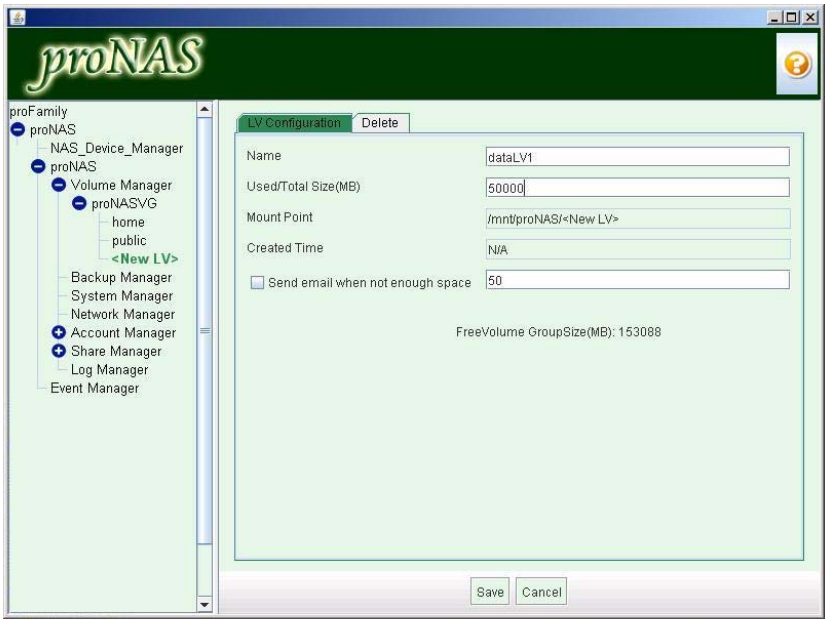
Disk List (Total: 1)

Dele...	Stat...	Disk...	Size...
□	IN_USED	/dev/sda	156897

Volume List (Total: 2)

Volume	Size(MB)	Used Size(MB)	Rep. Enable
home	512	4	No
public	512	4	No

2. The LV Configuration tab will be displayed. Enter the Logical Volume name and the volume size (in MB). You can also enable the “Send email when not enough space” option to send an email notification to email recipients specified in Event Manager if the remaining free volume size is smaller than the size entered in this option. Click “Save” when done.



Name: dataLV1

Used/Total Size(MB): 50000

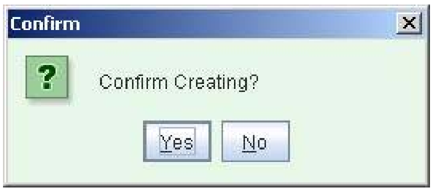
Mount Point: /mnt/proNAS/<New LV>

Created Time: N/A

□ Send email when not enough space: 50

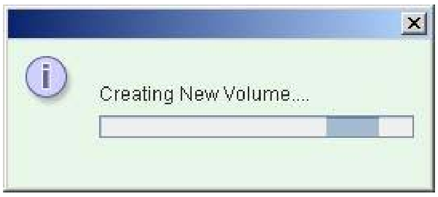
FreeVolume GroupSize(MB): 153088

3. Select “Yes” from the confirmation message to create the LV.



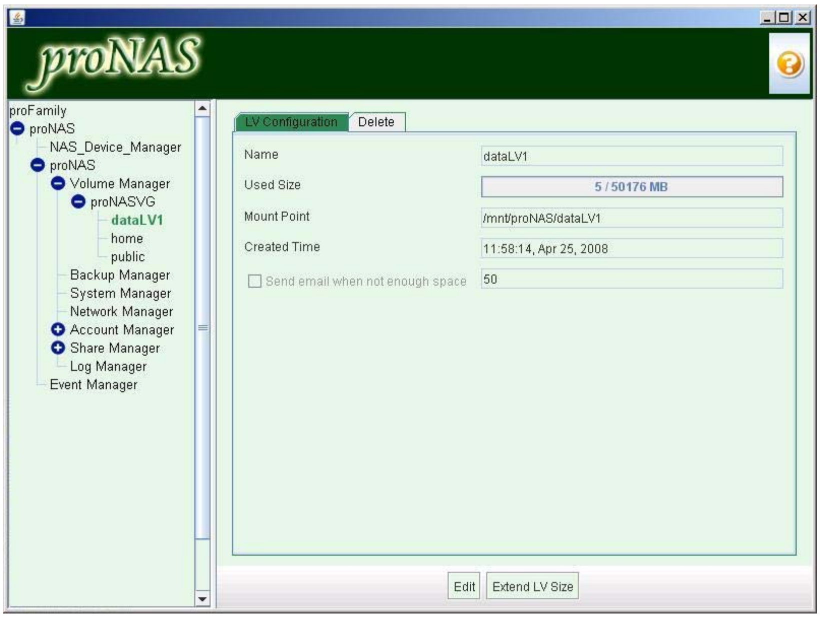
Confirm Creating?

4. A process window will be shown.



Creating New Volume....

5. The new Logical Volume will be shown.

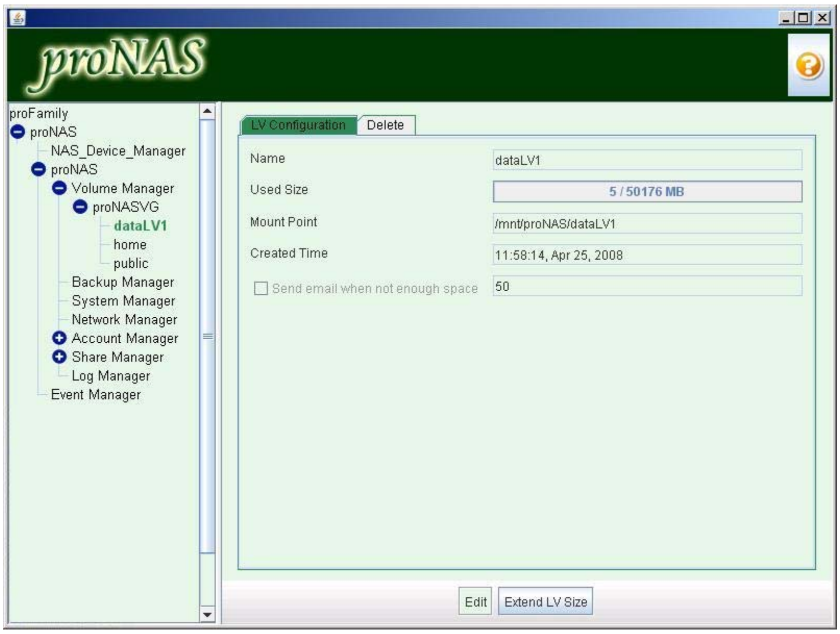


Name	dataLV1
Used Size	5 / 50176 MB
Mount Point	/mnt/proNAS/dataLV1
Created Time	11:58:14, Apr 25, 2008
□ Send email when not enough space	50

5.1.2.2 Extending Logical Volume Size

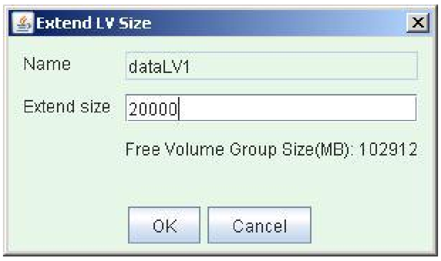
When the Logical Volume free space gets smaller and smaller, the Logical Volume size can be extended to allow more space for storing data. To extend the LV size, follow these steps:

1. Select the LV that will be extended then click "Extend LV Size" button.



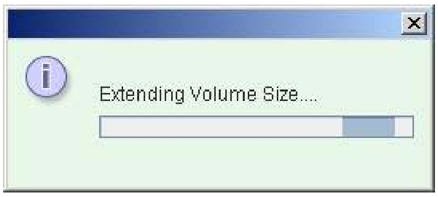
Name dataLV1
Used Size 5 / 50176 MB
Mount Point /mnt/proNAS/dataLV1
Created Time 11:58:14, Apr 25, 2008
□ Send email when not enough space 50

2. Enter in the "Extend size" box the additional size to be used for extension. Verify from the Free Volume Group Size (MB) the allowable size to be used in extension.



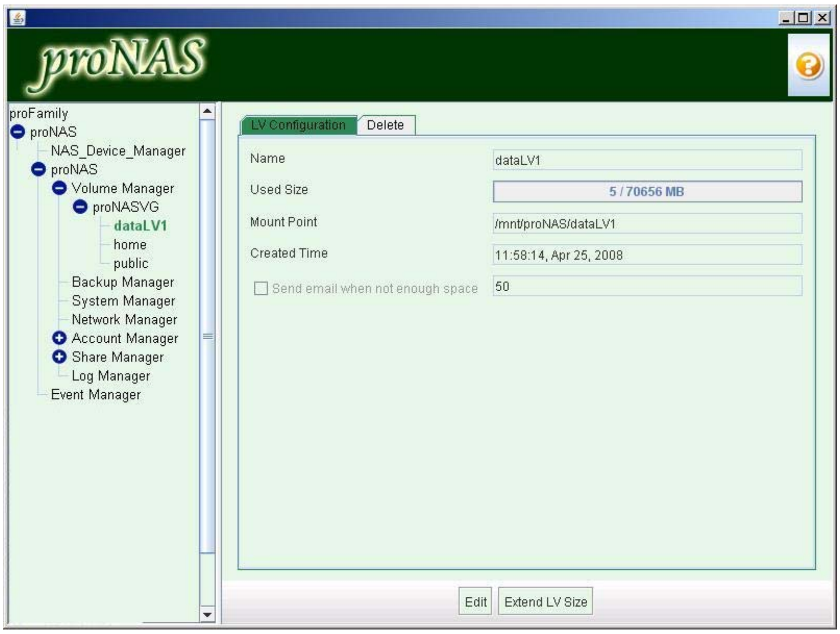
Name dataLV1
Extend size 20000
Free Volume Group Size(MB): 102912

3. The Logical Volume will be extended.



Extending Volume Size....

4. Verify the new LV size.



Name: dataLV1

Used Size: 5 / 70656 MB

Mount Point: /mnt/proNAS/dataLV1

Created Time: 11:58:14, Apr 25, 2008

□ Send email when not enough space: 50

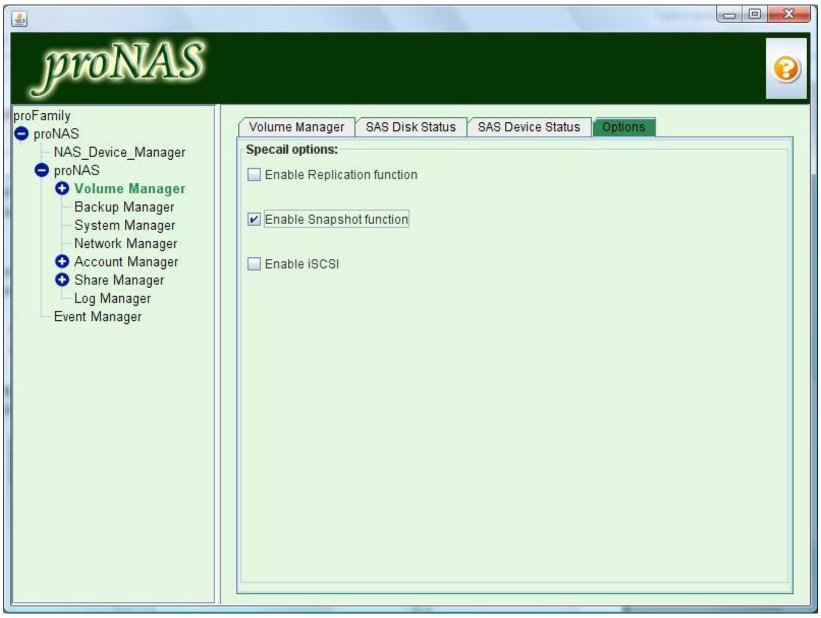
5.1.3 Volume Snapshot

Snapshots are point-in-time copies of a logical volume. This allows the system administrator to create a new block device which presents an exact copy of a logical volume, frozen at some point in time. As changes are made to the original volume, the snapshot remains the same and looks exactly like the original at the time the snapshot was created.

A Snapshot can be created manually or scheduled. Admin need to enable first this special function.

NOTE: Logical Volume with snapshot cannot be extended nor replicated (see next section about Volume Replication).

To enable Snapshot function, select Volume Manager then click Options tab. Tick the "Enable Snapshot function" option.



Specail options:

□ Enable Replication function

☑ Enable Snapshot function

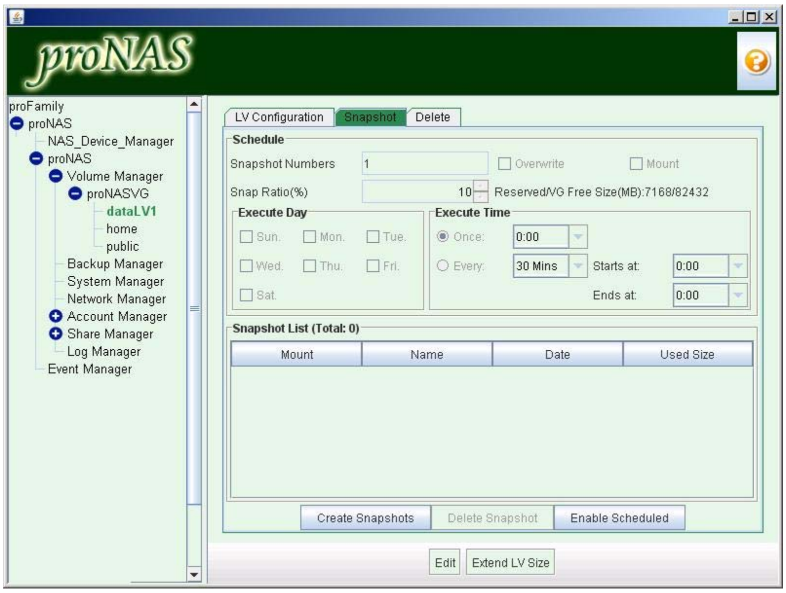
□ Enable iSCSI

NOTE: Creating Snapshots while a Logical Volume is under heavy I/O will slowdown the I/O access or interrupt the I/O process to a Logical Volume.

5.1.3.1 Create Snapshots Manually

To manually create snapshots:

1. Select the Logical Volume, go to Snapshot tab and click “Create Snapshot”.



Schedule

Snapshot Numbers 1 □ Overwrite □ Mount

Snap Ratio(%) 10 Reserved/VG Free Size(MB):7168/82432

Execute Day

□ Sun. □ Mon. □ Tue.
□ Wed. □ Thu. □ Fri.
□ Sat.

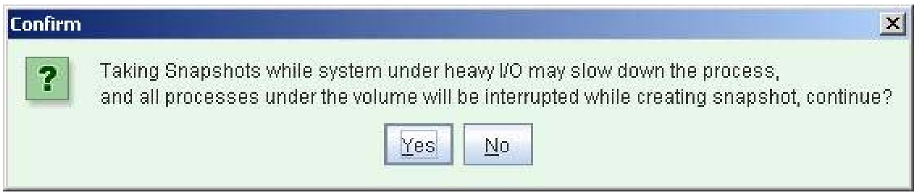
Execute Time

● Once: 0:00
○ Every: 30 Mins Starts at: 0:00
Ends at: 0:00

Snapshot List (Total: 0)

Mount	Name	Date	Used Size

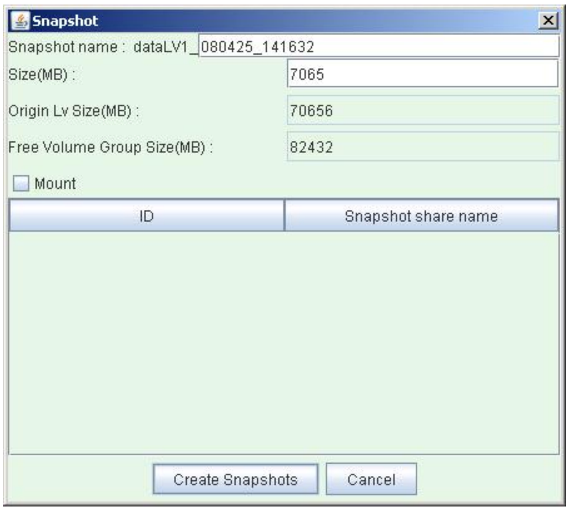
2. A confirmation message will appear. Select “Yes”.



Confirm

Taking Snapshots while system under heavy I/O may slow down the process,
and all processes under the volume will be interrupted while creating snapshot, continue?

3. The Snapshot configuration window will be displayed. A system-created Snapshot name is automatically created. The default snapshot name can be renamed if needed. Enter the new Snapshot Size (in MB) if the size shown need to be changed. See details about Snapshot Options below. Click “Create Snapshots” to start creating snapshot.



Snapshot

Snapshot name : dataLV1_080425_141632

Size(MB) : 7065

Origin Lv Size(MB) : 70656

Free Volume Group Size(MB) : 82432

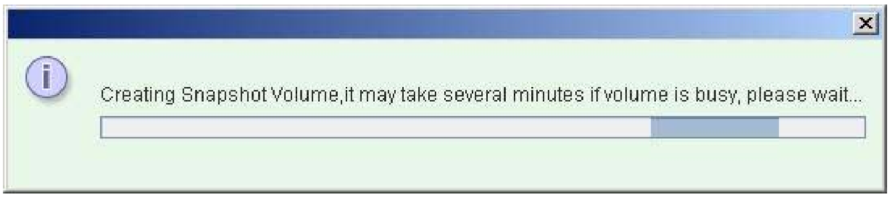
□ Mount

ID	Snapshot share name

Snapshot Options:

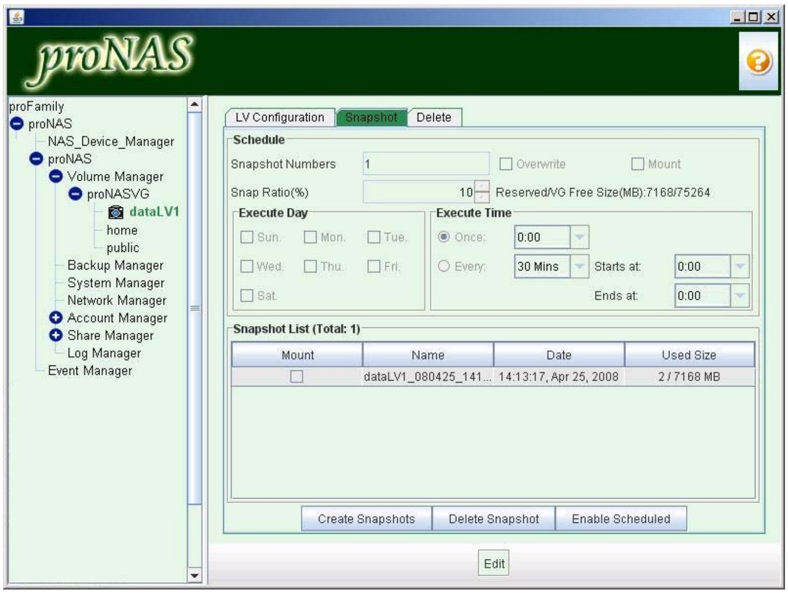
- **Snapshot Name:** The default snapshot name is created by appending the date and time to the volume name. You can modify the snapshot name but the prefix volume name will still remain.
- **Size (MB):** This indicates the size of the snapshot volume that will be created. The default is 10% of the size of the logical volume where snapshot is to be taken. The size of the snapshot volume will be multiple of the PE size.
- **Origin LV Size:** This indicates the size of the Logical Volume where the new snapshot volume will be created.
- **Free Volume Group Size (MB):** This indicates the amount of free space on the volume group where the new snapshot volume will be created.
- **Mount:** When checked, the created snapshot volume will be automatically mounted. When a snapshot volume is mounted, the existing share from the snapshot volume will be accessible. Note that a snapshot volume is a read-only volume.
- **ID:** This specifies the shares created under this logical volume.
- **Snapshot share name:** This specifies the name of the snapshot shares. Your may access these shares by mounting the snapshot volume. The naming format used is: the last two digit of the year, followed by the month/date, and then followed by the hour/min/sec. For example: "060123_171516".

4. A process window will be displayed.



Creating Snapshot Volume,it may take several minutes if volume is busy, please wait...

5. When snapshot has been created, it will be shown in the Snapshot List of the Logical Volume.



Schedule

Snapshot Numbers 1 □ Overwrite □ Mount

Snap Ratio(%) 10 Reserved/VG Free Size(MB):7168/75264

Execute Day: □ Sun. □ Mon. □ Tue. □ Wed. □ Thu. □ Fri. □ Sat.

Execute Time: ● Once: 0:00 ○ Every: 30 Mins Starts at: 0:00 Ends at: 0:00

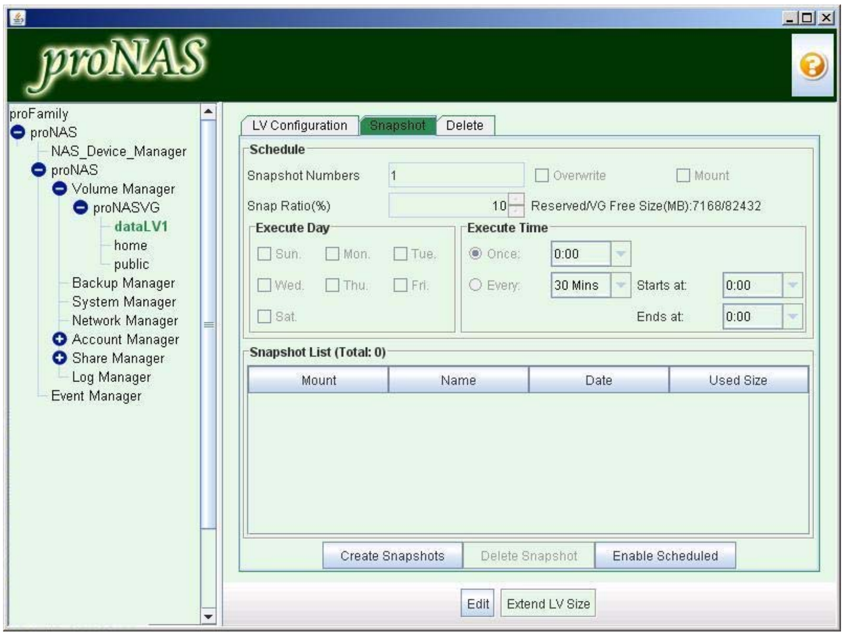
Snapshot List (Total: 1)

Mount	Name	Date	Used Size
□	dataLV1_080425_141...	14:13:17, Apr 25, 2008	2 / 7168 MB

5.1.3.2 Create Snapshots Based from Schedule

To create scheduled snapshots:

1. Select the Logical Volume, go to Snapshot tab and click “Edit”.



Schedule

Snapshot Numbers: 1 — □ Overwrite — □ Mount

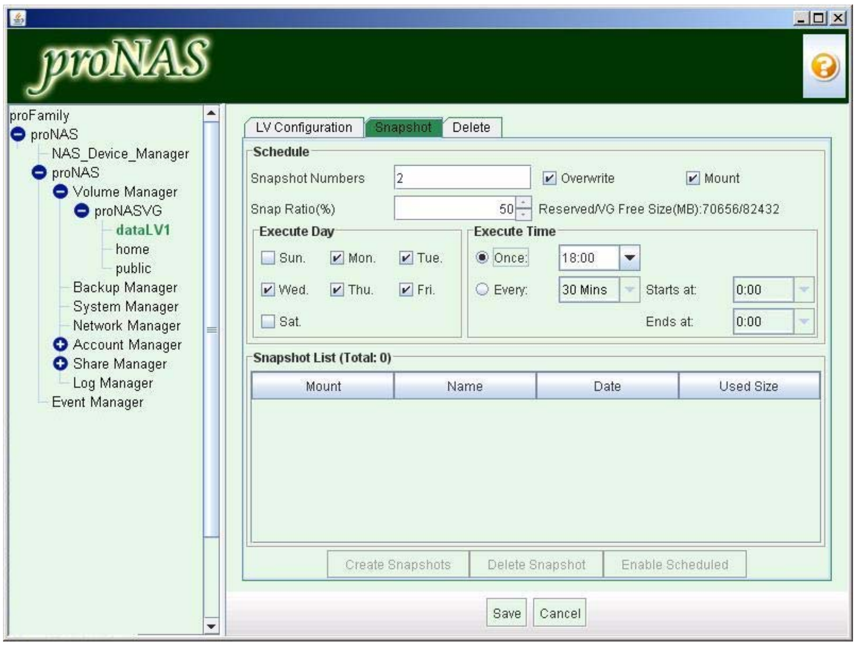
Snap Ratio(%): 10 — Reserved/VG Free Size(MB):7168/82432

Execute Day: □ Sun. □ Mon. □ Tue. □ Wed. □ Thu. □ Fri. □ Sat.

Execute Time: ● Once: 0:00 — ○ Every: 30 Mins — Starts at: 0:00 — Ends at: 0:00

Snapshot List (Total: 0)

2. Edit the following snapshot options listed below then click “Save” when done.



Schedule

Snapshot Numbers: 2 — ☑ Overwrite — ☑ Mount

Snap Ratio(%): 50 — Reserved/VG Free Size(MB):70656/82432

Execute Day: □ Sun. ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. □ Sat.

Execute Time: ● Once: 18:00 — ○ Every: 30 Mins — Starts at: 0:00 — Ends at: 0:00

Snapshot List (Total: 0)

Snapshot Options:

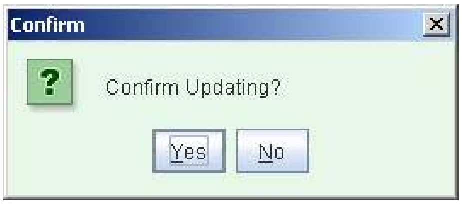
- **Snapshot Numbers:** Specifies the total number of snapshots that will be created.
- **Snap Ratio (%):** This is the ratio in percentage between the snapshot volume and the volume of origin. This indicates the ratio of the volume size that will be set as the size of the snapshot volume. For example, if your logical volume is 1GB and the Snap Ratio is 10%, the size of the snapshot volume that will be created is 128MB, assuming that your PE size is 128MB and below. The snapshot volume size will always be a multiple of PE size and the smallest snapshot size is equal to the PE size.
- **Overwrite:** Selecting this option will automatically delete the oldest snapshot if the total number of snapshots is already exceeded.
- **Mount:** When checked, it means that the created scheduled snapshot will be automatically mounted.
- **Reserved/VG Free Size (MB):** The left side indicates the total volume space that will be used for the creation the snapshots. The right side indicates the free space of the volume group available for use.
- **Execute Day:** Specifies whether the scheduled task is to run on the selected day(s).
- **Execute time:**

  Once - Specifies the time of the day when the scheduled task will be taken.
  Every - Specifies how often the scheduled task is to be repeated. You can also select the starting time and the ending time.

- **Snapshot Lists:**

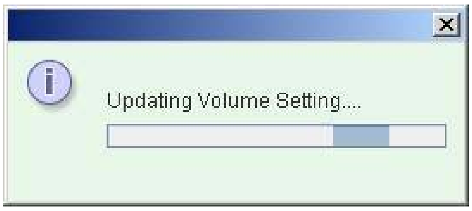
  Mount - Allows you to mount the snapshot volume. All snapshot volumes will be mounted read-only. By mounting the snapshot volume, the files under this snapshot volume will become accessible.
  Name - This specifies the name of the snapshot volume. If the snapshots are created by schedule, proNAS will automatically create the snapshot name. The format that will be used is: the last two digit of the year, followed by the month/date, and then followed by the hour/min/sec. For example: "060123_171516".
  Date - This indicates the date and time when the snapshot was created.
  Used Size - This indicates the space used by the snapshot data. The right side is the size of the snapshot volume. If the used space nearly exceeds the snapshot volume capacity, it will be set as "Invalid" and will be un-mounted automatically to keep the system consistent.

3. A confirm message window will be displayed. Select “Yes” to proceed.



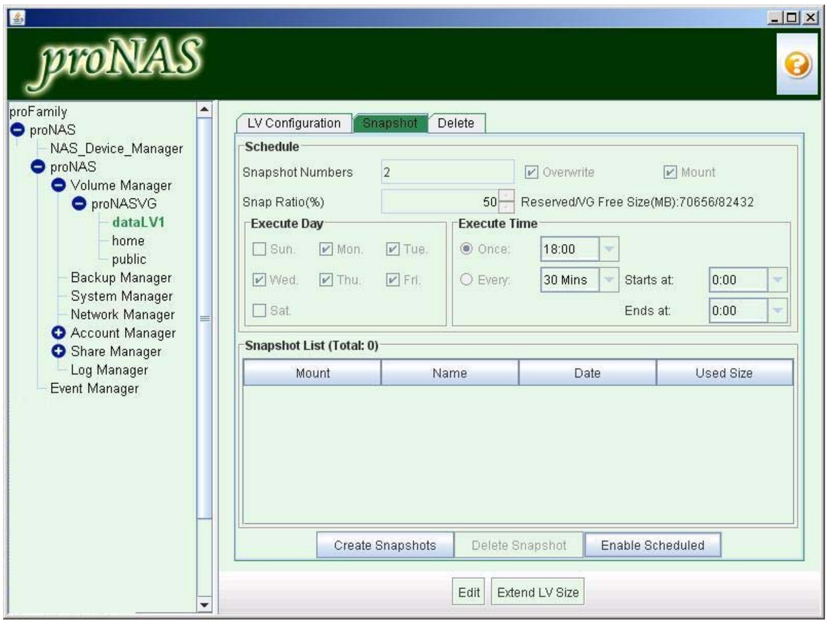
Confirm Updating?

4. An “Updating Volume Setting” message will be shown.



Updating Volume Setting....

5. When the snapshot setting of LV has been set, click “Enable Scheduled” to active scheduled snapshot.



Schedule

Snapshot Numbers: 2 ☑ Overwrite ☑ Mount

Snap Ratio(%): 50 Reserved/VG Free Size(MB):70656/82432

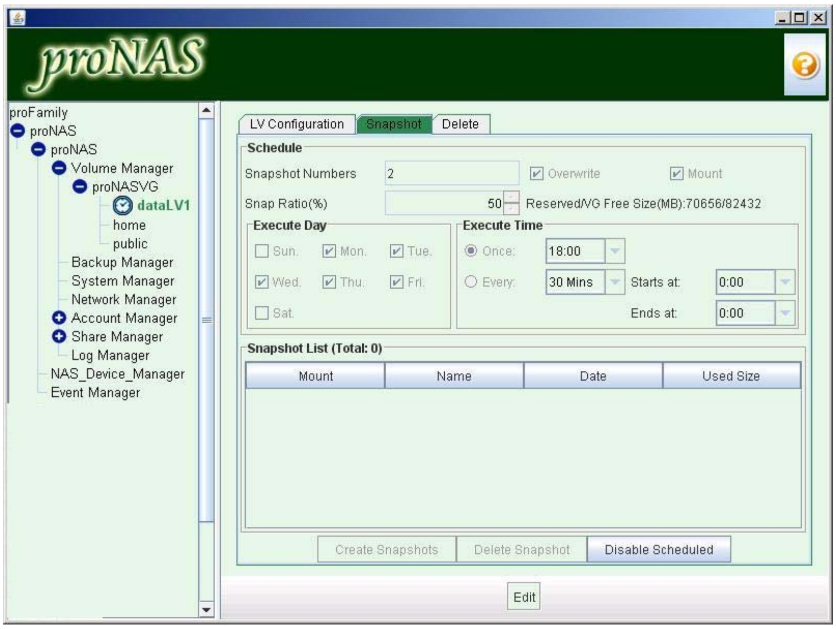
Execute Day: □ Sun. ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. □ Sat.

Execute Time: ● Once: 18:00 ○ Every: 30 Mins Starts at: 0:00 Ends at: 0:00

Snapshot List (Total: 0)

Mount	Name	Date	Used Size

6. A clock-like icon will appear on the left side of the LV which means a scheduled snapshot is active. To disable the schedule, click “Disable Scheduled”.



Schedule

Snapshot Numbers: 2 ☑ Overwrite ☑ Mount

Snap Ratio(%): 50 Reserved/VG Free Size(MB):70656/82432

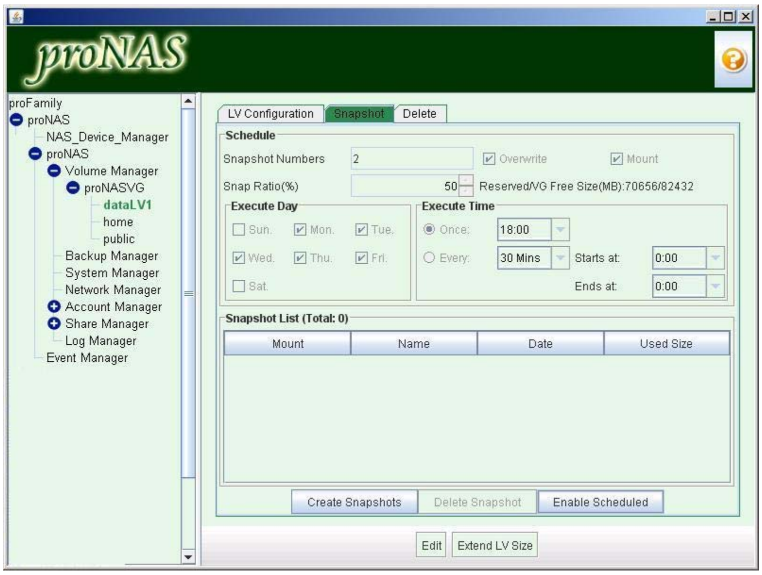
Execute Day: □ Sun. ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. □ Sat.

Execute Time: ● Once: 18:00 ○ Every: 30 Mins Starts at: 0:00 Ends at: 0:00

Snapshot List (Total: 0)

Mount	Name	Date	Used Size

7. After disabling the schedule, the “Enable Scheduled” button will become available.



Schedule

Snapshot Numbers 2 ☑ Overwrite ☑ Mount

Snap Ratio(%) 50 Reserved/VG Free Size(MB):70656/82432

Execute Day: ☐ Sun. ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thu. ☑ Fri. ☐ Sat.

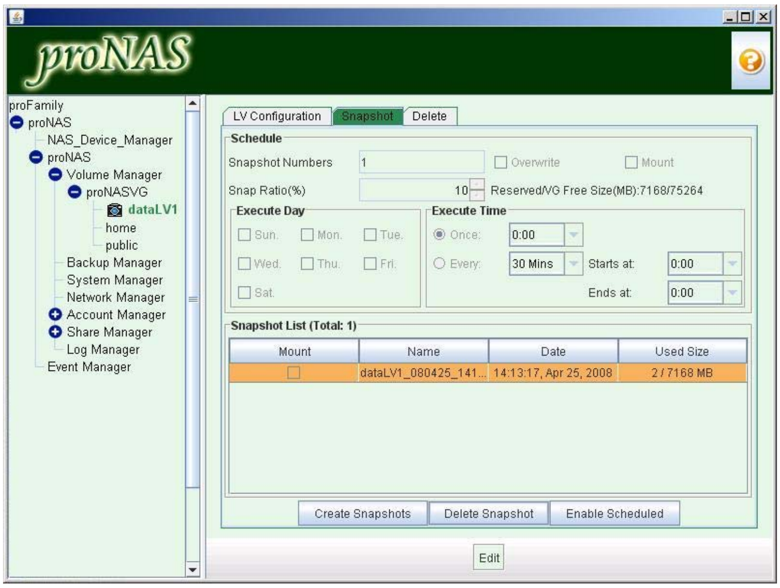
Execute Time: ● Once: 18:00 ○ Every: 30 Mins Starts at: 0:00 Ends at: 0:00

Snapshot List (Total: 0)

Mount	Name	Date	Used Size

5.1.3.3 Delete Snapshots

1. Select the Logical Volume where snapshot will be deleted, then go to Snapshot tab. Click the snapshot that will be deleted then click “Delete Snapshot”.



Schedule

Snapshot Numbers 1 ☐ Overwrite ☐ Mount

Snap Ratio(%) 10 Reserved/VG Free Size(MB):7168/75264

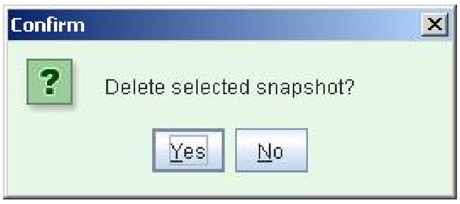
Execute Day: ☐ Sun. ☐ Mon. ☐ Tue. ☐ Wed. ☐ Thu. ☐ Fri. ☐ Sat.

Execute Time: ● Once: 0:00 ○ Every: 30 Mins Starts at: 0:00 Ends at: 0:00

Snapshot List (Total: 1)

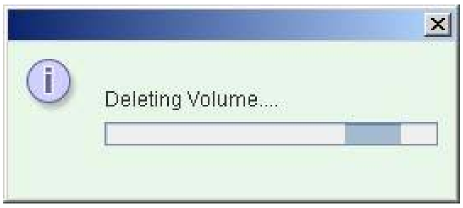
Mount	Name	Date	Used Size
☐	dataLV1_080425_141...	14:13:17, Apr 25, 2008	2 / 7168 MB

2. Select “Yes” to delete the snapshot.



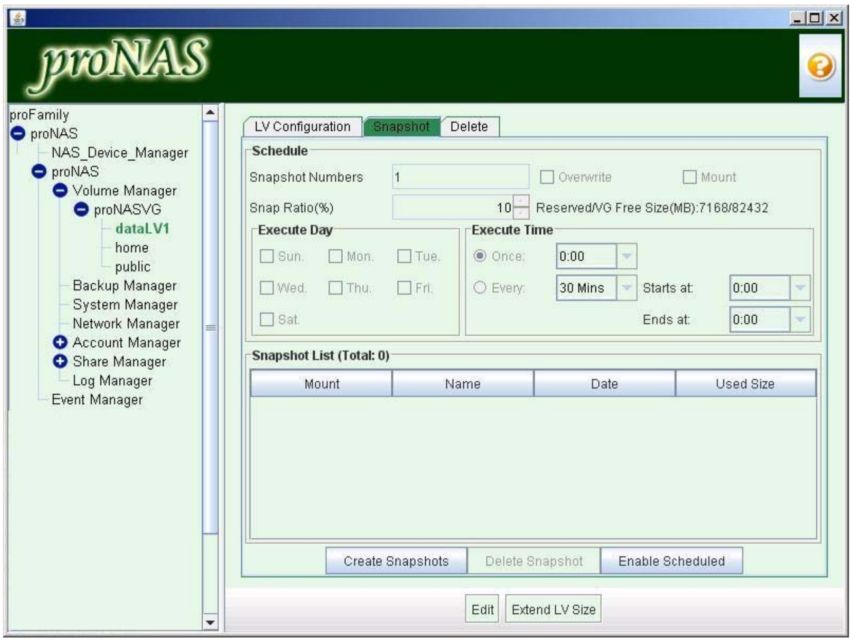
Delete selected snapshot?

3. A process window will be shown.



Deleting Volume....

4. The deleted snapshot will no longer exist in the Snapshot List.



Schedule

Snapshot Numbers 1 □ Overwrite □ Mount

Snap Ratio(%) 10 Reserved/VG Free Size(MB):7168/82432

Execute Day

□ Sun. □ Mon. □ Tue.

□ Wed. □ Thu. □ Fri.

□ Sat.

Execute Time

● Once: 0:00

○ Every: 30 Mins Starts at: 0:00

Ends at: 0:00

Snapshot List (Total: 0)

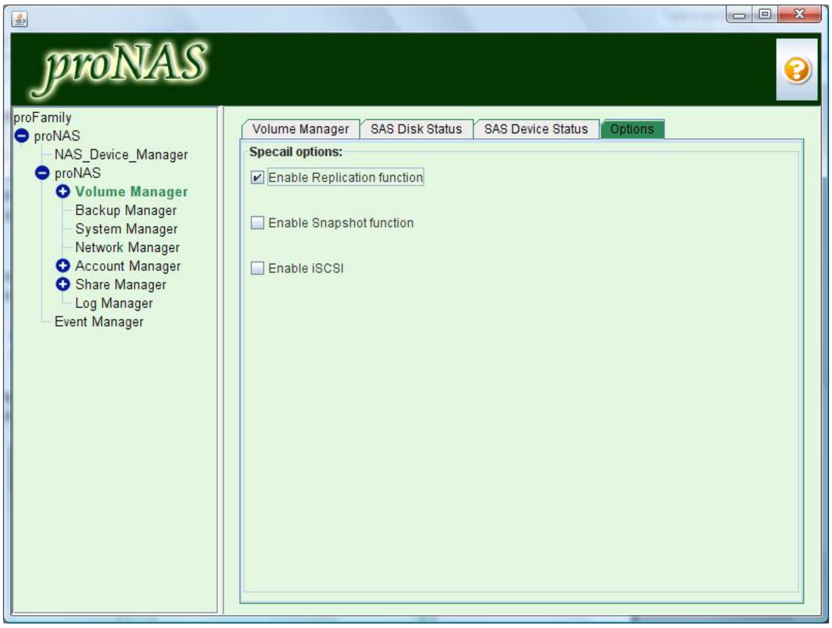
Mount	Name	Date	Used Size

5.1.4 Volume Replication

Replication function enables proNAS to replicate a logical volume from one NAS server (source) to another NAS server (destination). Replication involves intelligent copying and maintaining of exact copy of a volume from a source server to a destination server. The destination volume is always an exact copy of the source volume. This is done by mirroring the whole block device via a standard network interface. This solution creates a real time replication of data. However, it does not create a cluster solution where you can have a highly available system.

Note: Logical Volume under snapshot cannot be replicated.

To enable Replication, select Volume Manager then click Options tab and tick “Enable Replication function”.



Specail options:

☑ Enable Replication function

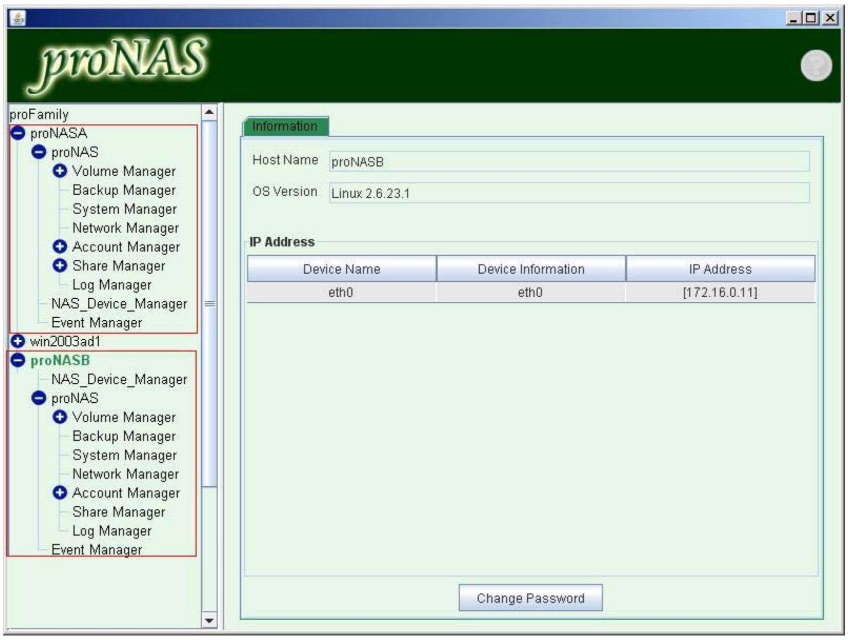
□ Enable Snapshot function

□ Enable iSCSI

5.1.4.1 Replication Configuration

To setup Replication between two NAS servers:

1. Admin need to login to the administration page of the two NAS servers.



- proFamily
  - proNASA
    - proNAS
      - Volume Manager
      - Backup Manager
      - System Manager
      - Network Manager
      - Account Manager
      - Share Manager
      - Log Manager
    - NAS_Device_Manager
    - Event Manager
  - win2003ad1
  - proNASB
    - NAS_Device_Manager
    - proNAS
      - Volume Manager
      - Backup Manager
      - System Manager
      - Network Manager
      - Account Manager
      - Share Manager
      - Log Manager
    - Event Manager

Information

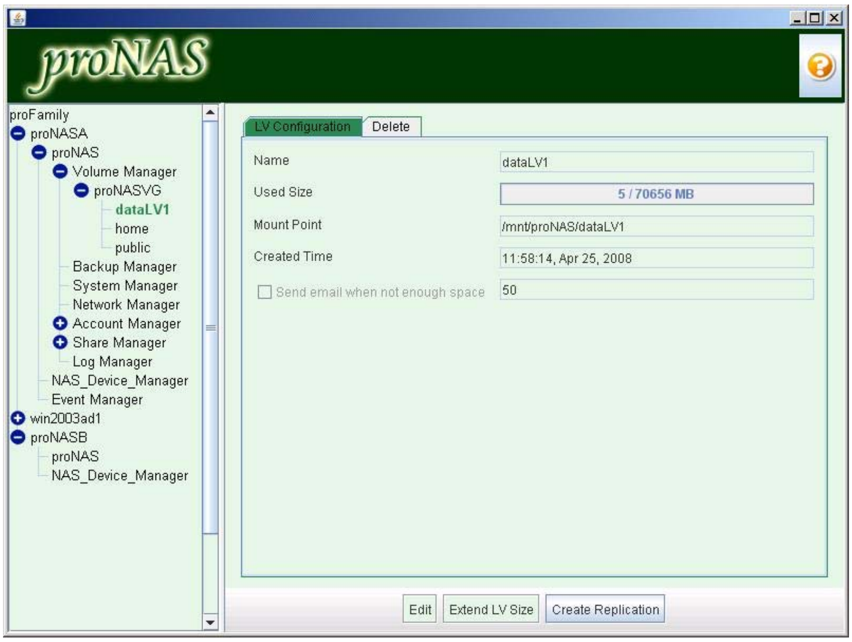
Host Name: proNASB

OS Version: Linux 2.6.23.1

IP Address

Device Name	Device Information	IP Address
eth0	eth0	[172.16.0.11]

2. On the primary NAS (source), select the Logical Volume which will be replicated, then click “Create Replication”.



- proFamily
  - proNASA
    - proNAS
      - Volume Manager
        - proNASVG
          - dataLV1
          - home
          - public
      - Backup Manager
      - System Manager
      - Network Manager
      - Account Manager
      - Share Manager
      - Log Manager
    - NAS_Device_Manager
    - Event Manager
  - win2003ad1
  - proNASB
    - proNAS
    - NAS_Device_Manager

LV Configuration | Delete

Name: dataLV1

Used Size: 5 / 70656 MB

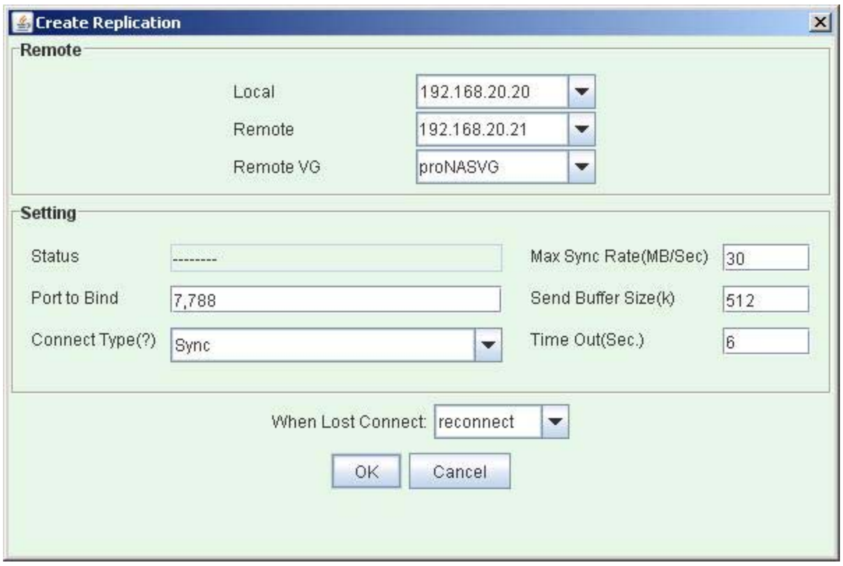
Mount Point: /mnt/proNAS/dataLV1

Created Time: 11:58:14, Apr 25, 2008

□ Send email when not enough space: 50

NOTE: The logical volume to be replicated from source proNAS must not exist in the destination proNAS. If the destination proNAS has the same logical volume, replication cannot be setup.

3. The Create Replication window will be displayed. Set the options below and click "OK" when done.



Local: 192.168.20.20
Remote: 192.168.20.21
Remote VG: proNASVG

Status: --------
Port to Bind: 7,788
Connect Type(?): Sync
Max Sync Rate(MB/Sec): 30
Send Buffer Size(k): 512
Time Out(Sec.): 6

When Lost Connect: reconnect

Replication Options:

[Remote]

- **Local** - Select the IP address of the local (source) proNAS that will be used for replication.
- **Remote** - Select or type manually the IP address of remote (destination) proNAS that will be used for replication.

NOTE: The local and remote IP addresses serve as the channel between the source and destination NAS servers. This is where the replication of data takes place. Please be sure to have a good connection on this medium. As much as possible, set this channel as a dedicated or a private network. It is recommended to use different Ethernet port for replication from the Ethernet port used for data access. It is best to use a crossover network link between the Ethernet ports involved. Refer to Network Manager Section for configuring Ethernet port.

- **Remote VG** - Select the VG on remote proNAS where the replicated logical volume will be created.

[Setting]

- **Port to Bind** - A TCP port to bind locally and is used to connect to the remote node. Default is 7788.

  NOTE: User cannot use ports that already have been used. Available ports are from 7788 to 77xx.

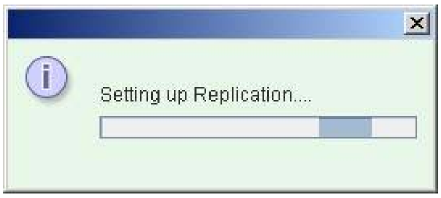
- **Connection Type:** proNAS supports two types of data replication protocols:
  - **Sync** - Synchronous. The system will acknowledge the transaction as completed after the data is written to the disk of destination proNAS. It is recommended to use this mode. In most cases, this connection type preserves transaction semantics. Write IO is reported as completed if it has reached the remote disk.
  - **Async** (for high latency network) - Asynchronous. The system will acknowledge the transaction as completed after the data is written to buffer. It provides faster transmission and is suitable for busy network. Write IO is reported as completed if it has reached the local TCP send buffer.
- **Max Sync Rate** – This sets the limit of the bandwidth that will be used by the synchronization process. Default is 30MB/sec. Minimum value is 4MB/sec and maximum value is 680 MB/sec – for high latency network environment (e.g. bonding on Gigabit Ethernet).
- **Send buffer size (K)** - It is the size of the TCP socket send buffer. You can specify smaller or larger values. Larger values are appropriate for reasonable write throughput with asynchronous protocol over high latency networks. Default is 512K and maximum is 1024K.
- **Time out (sec)** - It is the value to wait for connection timeout if the remote node is degraded. If the remote node fails to send the response packet within the specified timeout time, the remote node will be considered dead and the TCP/IP connection is abandoned. The default is 6 sec. Minimum is 1 sec and maximum is 60 sec.

- **When Lost Connection**: When the replication connection is lost, the replication program can either go stand-alone or will try to reconnect.

  - **Reconnect:** The replication program will attempt to reconnect. (Default)
  - **Stand-alone:** The replication program will not attempt to reconnect and will go on stand-alone state. All IO request are only passed locally and no replication.

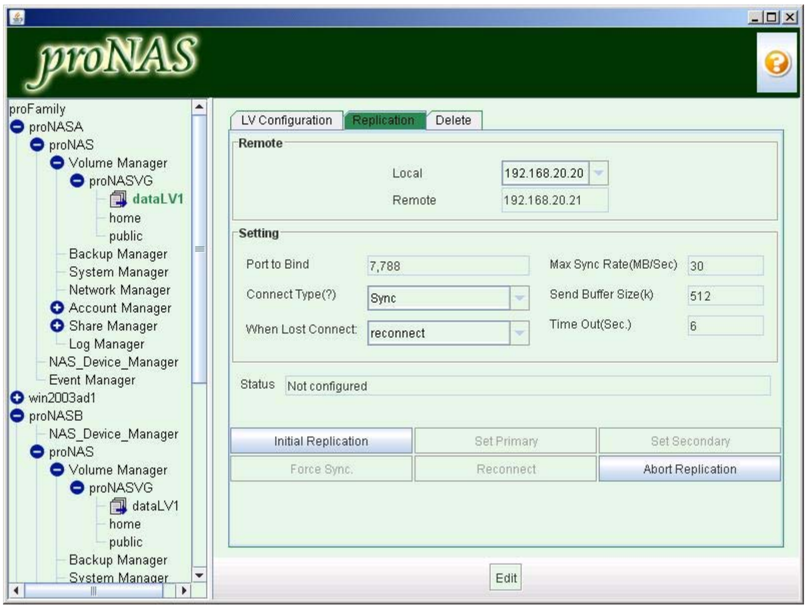
NOTE: Before replication will be successfully created, a 4GB logical volume will be created on each node. This will serve as the metadata device for the replicated volume. This volume is not mounted and will not be seen on the proNAS GUI. Please be sure to have an extra 4GB space on either side of your NAS nodes.

4. A message box will be displayed.



Setting up Replication....

5. Initialize the Replication by clicking “Initial Replication” button.



Remote

Local 192.168.20.20

Remote 192.168.20.21

Setting

Port to Bind 7,788

Max Sync Rate(MB/Sec) 30

Connect Type(?) Sync

Send Buffer Size(k) 512

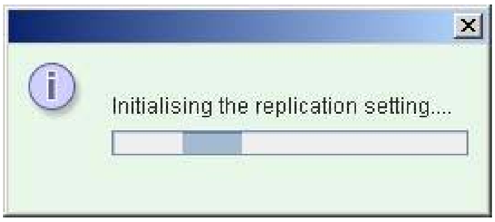
When Lost Connect reconnect

Time Out(Sec.) 6

Status Not configured

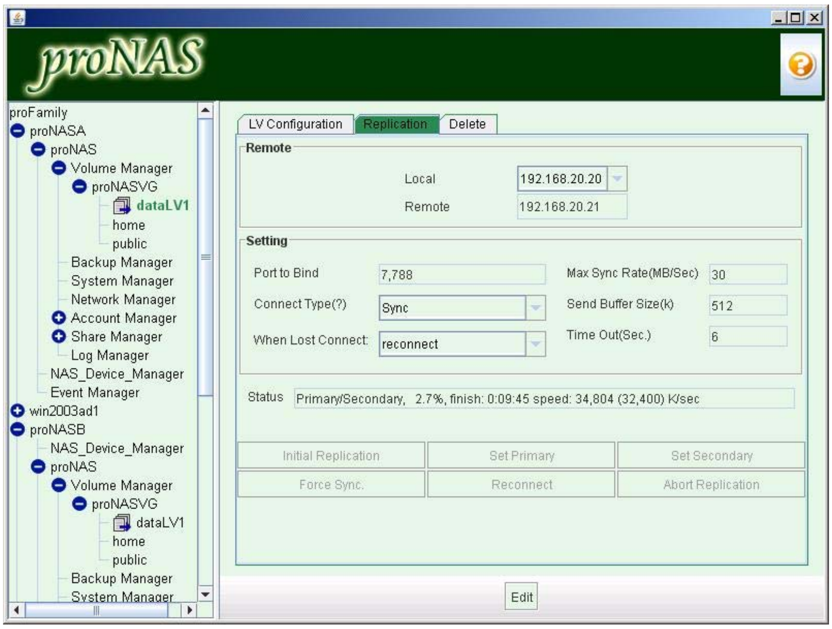
NOTE: After creating a replication, a similar logical volume will be created on the destination server under the specified VG. At this point, the replication is not yet initialized and no synchronization. Replication still needs to be initialized. After selecting “Initial Replication”, the first node will then connect to the second node and starts to synchronize. Synchronization typically takes quite a while especially on larger logical volumes. After initializing, the source node should be in "Primary" state and the destination node should be in "Secondary" state. If this is the state, you have now a working replication. Initializing should be done in the source volume.

6. The volume replication setting will be initialized.



Initialising the replication setting....

7. The volume replication synchronization process will start.



Remote

Local 192.168.20.20

Remote 192.168.20.21

Setting

Port to Bind 7,788

Max Sync Rate(MB/Sec) 30

Connect Type(?) Sync

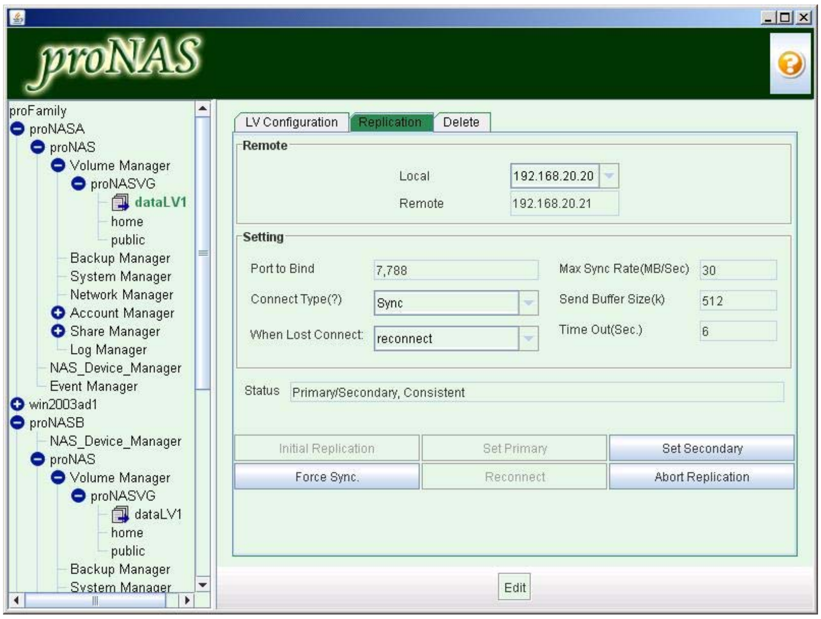
Send Buffer Size(k) 512

When Lost Connect reconnect

Time Out(Sec.) 6

Status Primary/Secondary, 2.7%, finish: 0:09:45 speed: 34,804 (32,400) K/sec

8. After the initial synchronization process is completed, the Status will show “Primary/Secondary Consistent”.



Remote

Local 192.168.20.20

Remote 192.168.20.21

Setting

Port to Bind 7,788

Max Sync Rate(MB/Sec) 30

Connect Type(?) Sync

Send Buffer Size(k) 512

When Lost Connect reconnect

Time Out(Sec.) 6

Status Primary/Secondary, Consistent

5.1.4.2 Checking the status of your replication

Primary: The source volume. All the writing and reading are done on the primary node.

Secondary: The destination volume. The replicated data on the secondary node is used for backup only and is not accessible. Only the source data is accessible during replication.

Unknown: The peer node fails to establish connection.

Setting the replicated volume on destination proNAS to be primary

To set the replicated volume to primary, first you need to set both nodes to secondary. This can be done by setting the primary to be secondary. After both nodes becomes secondary/secondary, go to the management GUI of the destination node. Under the replicated logical volume, press the "Set Primary" button.

WARNING! The replicated volume on the secondary node must not be mounted. Please do not attempt to mount it manually.

Setting the primary volume to be secondary

To set the primary volume to be secondary, just press the "Set Secondary" button on the primary node.

Forcing the synchronization

To manually force the synchronization, press the "Force Sync." button. The data on the primary node will be forcefully synchronized to the secondary node.

Reconnect when the connection of the peer is lost.

To reconnect the replicated volume, press the "Reconnect" button. At some point if the replication fails to establish connection to the other node, you may try to set up a connection thru this button. This button will be enabled only if one of the node losses connection.

Aborting the replication

To abort or drop the replication, press the "Abort Replication" button. To access the data on the replicated volume after aborting the replication, you may need to create a share under destination volume whose share name must be equal to the share name on the source proNAS.

5.1.4.3 Extending logical volume under replication

NOTE: Extending the size of a Logical Volume under replication is not allowed. However, there is a work around to extend the LV size. The following are the steps:

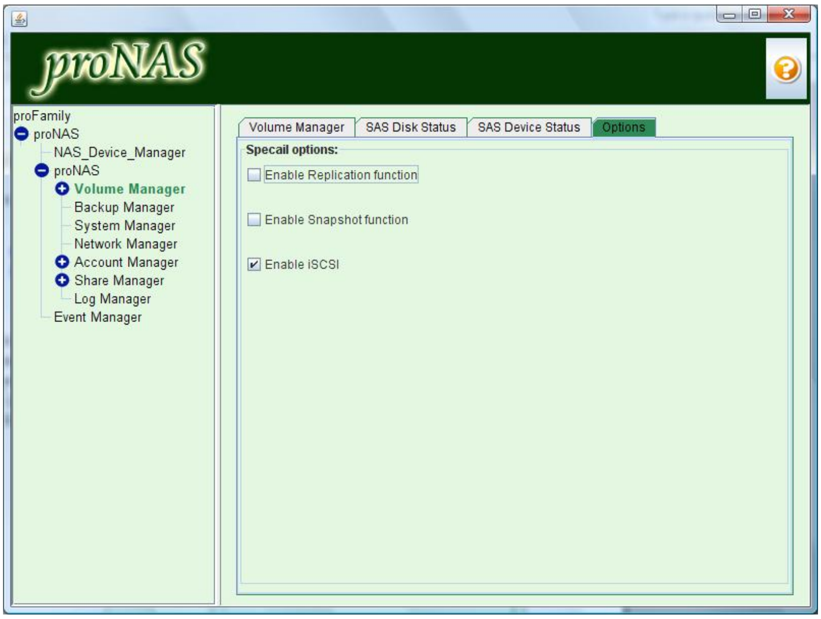
1. Abort the replication by selecting “Abort Replication”.
2. Remove or delete the replicated logical volume on the destination proNAS.
3. Extend the capacity of the source logical volume. Please note that there should be enough space on the logical volume of the destination proNAS to accommodate the extended logical volume space.
4. Create a new replication using the extended source logical volume.

5.1.5 iSCSI

The iSCSI function in proNAS makes a logical volume become an iSCSI target LUN.

Note: You can't enable iSCSI function in a Logical Volume if Snapshot or Replication exists.

To enable iSCSI function, select Volume Manager then click Options tab and tick "Enable iSCSI".



Specail options:

☐ Enable Replication function

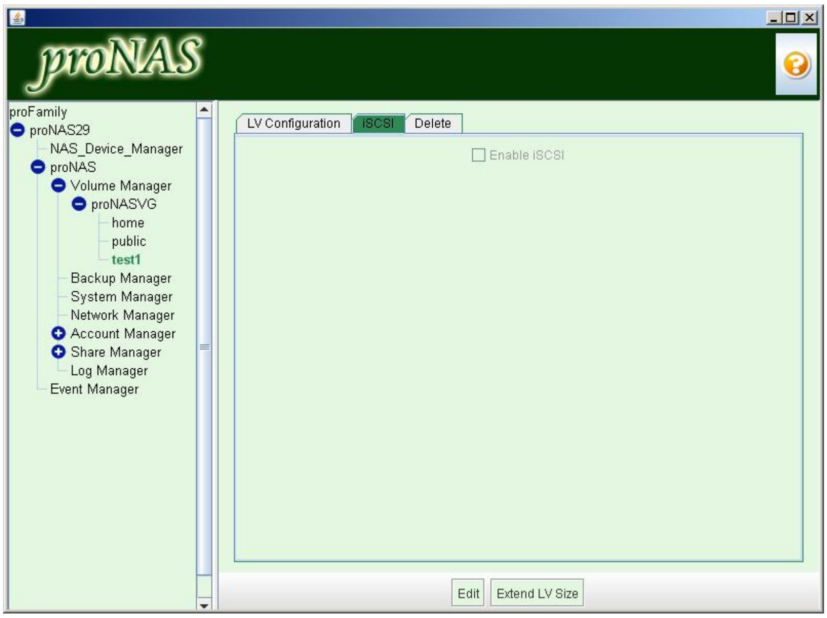
☐ Enable Snapshot function

☑ Enable iSCSI

5.1.5.1 iSCSI Configuration

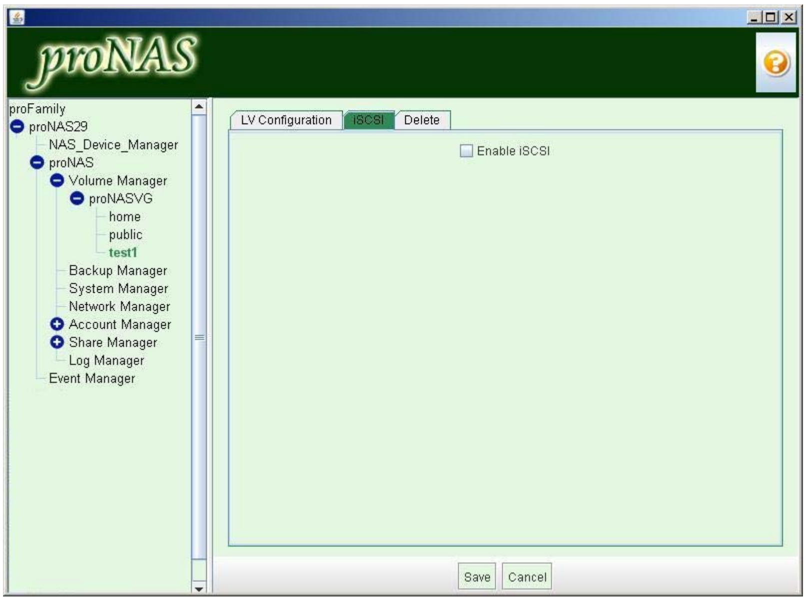
To configure iSCSI:

1. Select the logical volume and click the iSCSI tab.



☐ Enable iSCSI

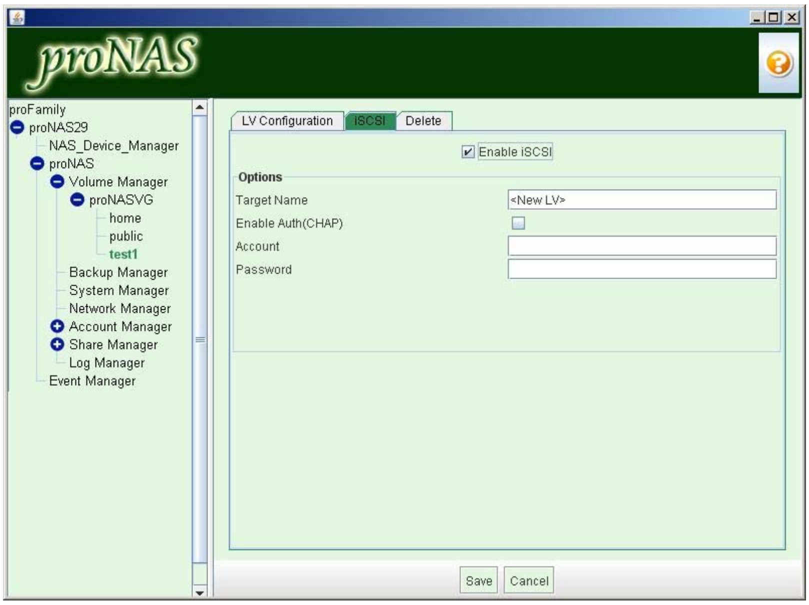
2. Click “Edit” and tick the “Enable iSCSI” option.



□ Enable iSCSI

3. Enter the target name. If you want to enable CHAP authentication, check the “Enable Auth (CHAP)” option and enter CHAP account and password.

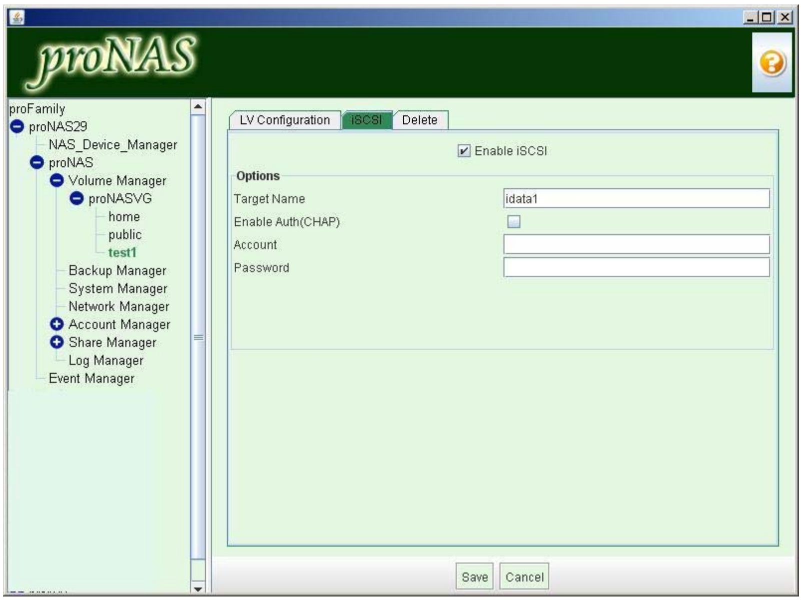
NOTE: Valid characters for Target Name are: a-z, A-Z, 0-9. Other special characters and space is not allowed. CHAP Password needs at least 12 characters.



☑ Enable iSCSI

Options

Target Name	<New LV>
Enable Auth(CHAP)	□
Account	
Password	



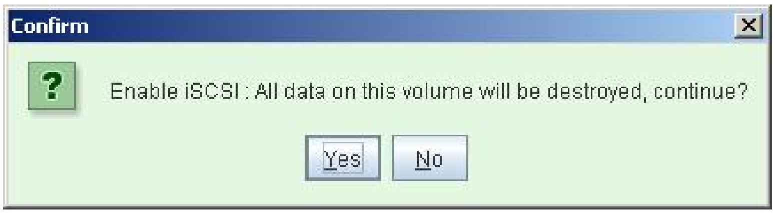
☑ Enable iSCSI

Options

Target Name	idata1
Enable Auth(CHAP)	□
Account	
Password	

4. Click “Save” when done.

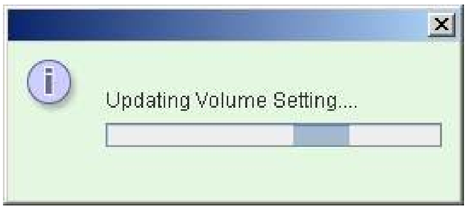
5. A message box will be displayed. Select “Yes” to continue.



Confirm

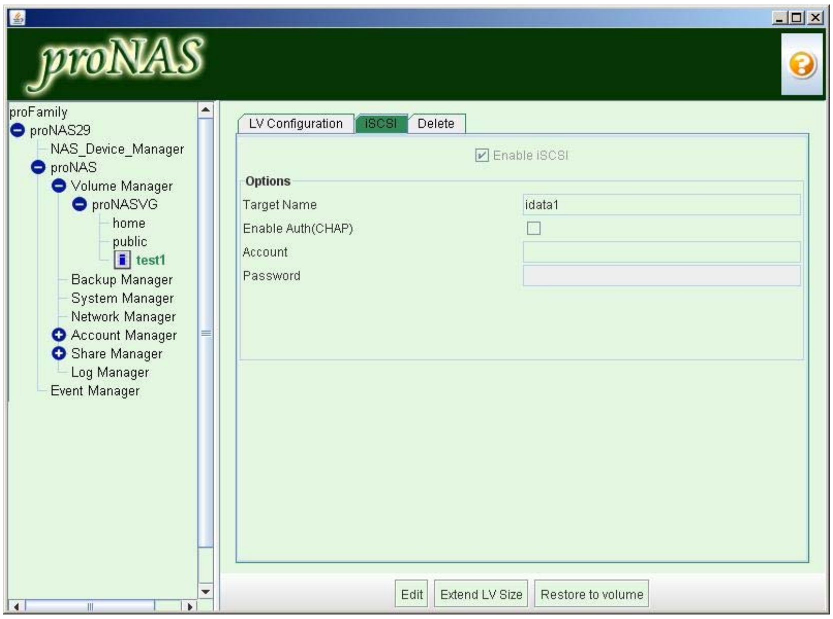
Enable iSCSI : All data on this volume will be destroyed, continue?

6. A progress box will be displayed.



Updating Volume Setting....

7. The iSCSI volume is ready. Note that there is an “**i**” icon on the left of logical volume name to denote that this is an iSCSI volume.



☑ Enable iSCSI

Options

Target Name	idata1
Enable Auth(CHAP)	☐
Account	
Password	

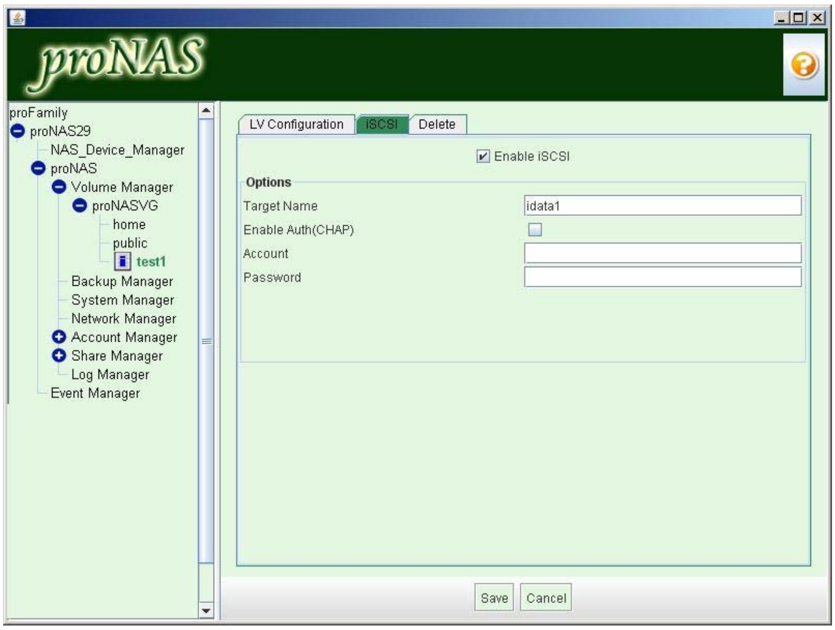
8. You may now connect to the iSCSI target LUN using iSCSI initiator.

5.1.5.2 Disable iSCSI in Logical Volume

To disable iSCSI:

1. Select the logical volume and click the iSCSI tab.

2. Click “Edit” and remove the check mark in “Enable iSCSI” option. Click “Save” when done.



☑ Enable iSCSI

Options

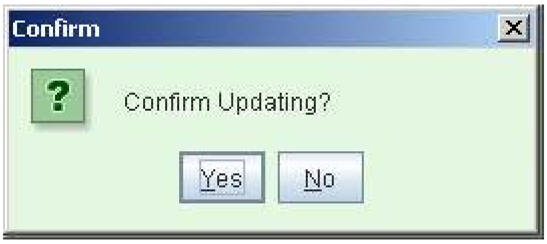
Target Name idata1

Enable Auth(CHAP) □

Account

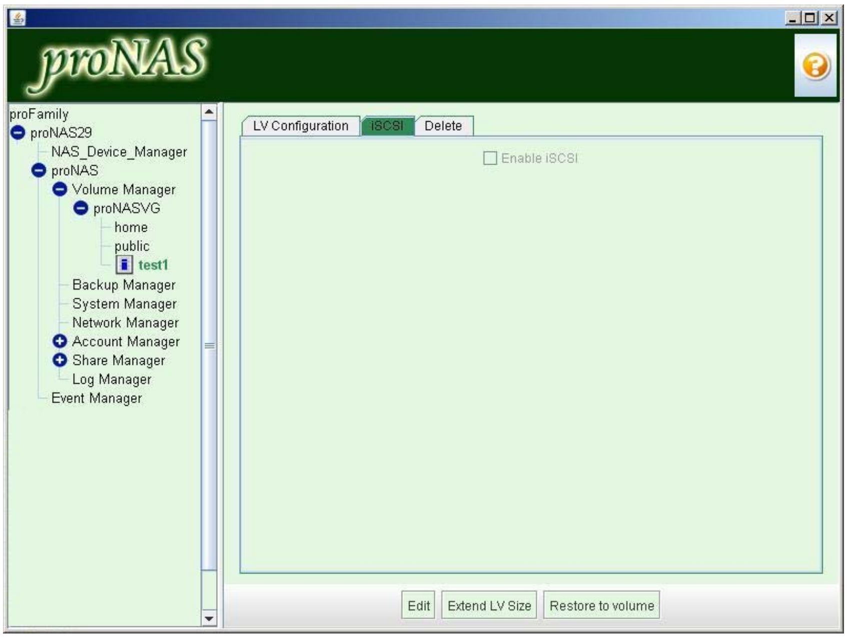
Password

3. A confirm message box will be displayed. Select “Yes” to proceed.



Confirm Updating?

4. The iSCSI function in the logical volume is disabled.



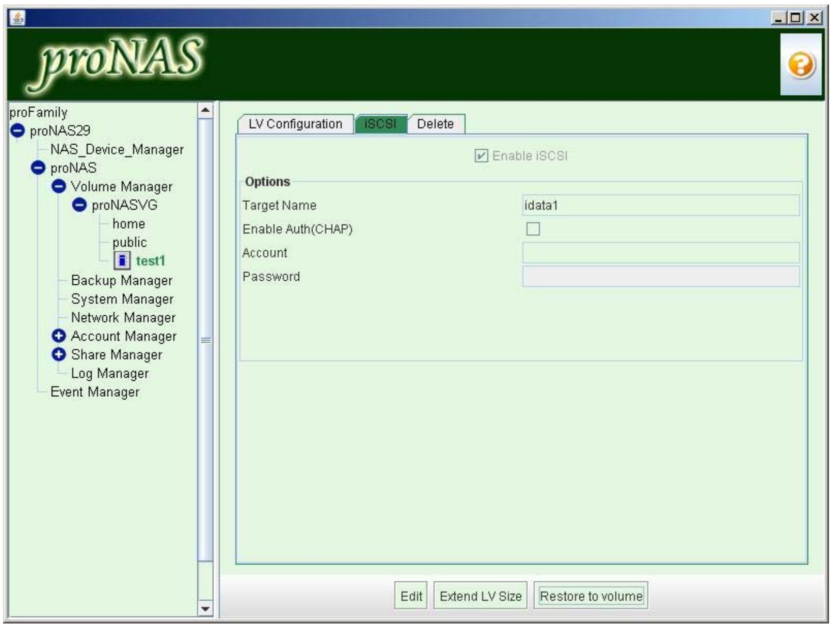
□ Enable iSCSI

5.1.5.3 Restore iSCSI to Ordinary Logical Volume

The iSCSI volume can be restored back to normal logical volume and remove the iSCSI function. The existing data in the logical volume will be deleted; so if there are important data in the logical volume, a backup must be made.

To restore iSCSI to normal volume:

1. Select the logical volume and click the iSCSI tab. Select the “Restore to Volume” button.



☑ Enable iSCSI

Options

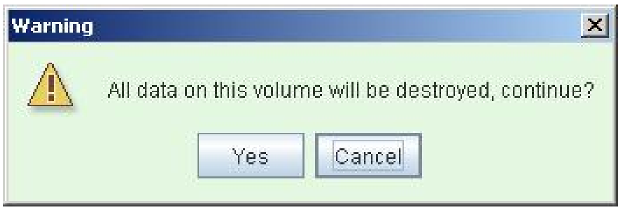
Target Name idata1

Enable Auth(CHAP) □

Account

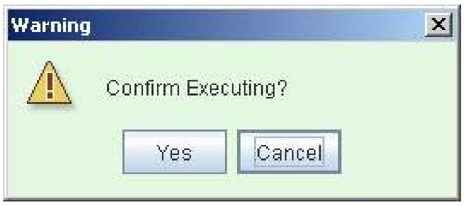
Password

2. When a warning message is displayed, select “Yes” to proceed.



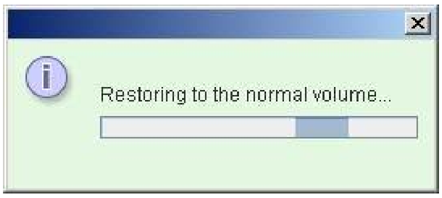
All data on this volume will be destroyed, continue?

3. When a confirm message is displayed, select “Yes”.



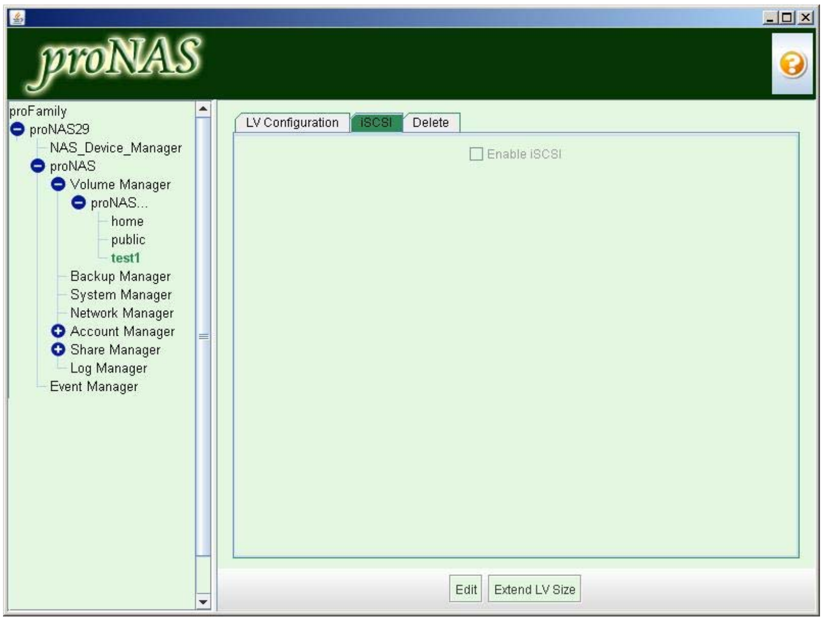
Confirm Executing?

4. A process window will show that the volume is being restored back to normal logical volume.



Restoring to the normal volume...

5. The logical volume is restored to normal volume. Note that the "**i**" icon on the left of logical volume name has been removed.



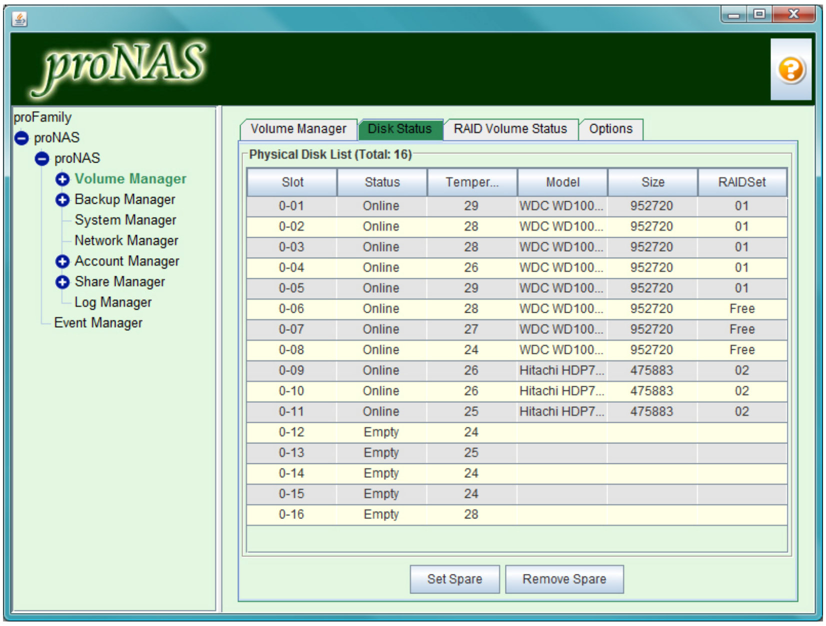
□ Enable iSCSI

5.1.6 SAS Disk Status and SAS Device Status

The proNAS GUI displays the SAS disk drives status, the Drive Group (RAID Set) and Virtual Drive (Volume Set), the power status, and the fan status.

5.1.6.1 SAS Disk Status

The SAS Disk Status screen will show the physical disk list, which disks are online, the slot temperature, the disk model, the disk size and the Drive Group or RAID Set the disk belongs to.



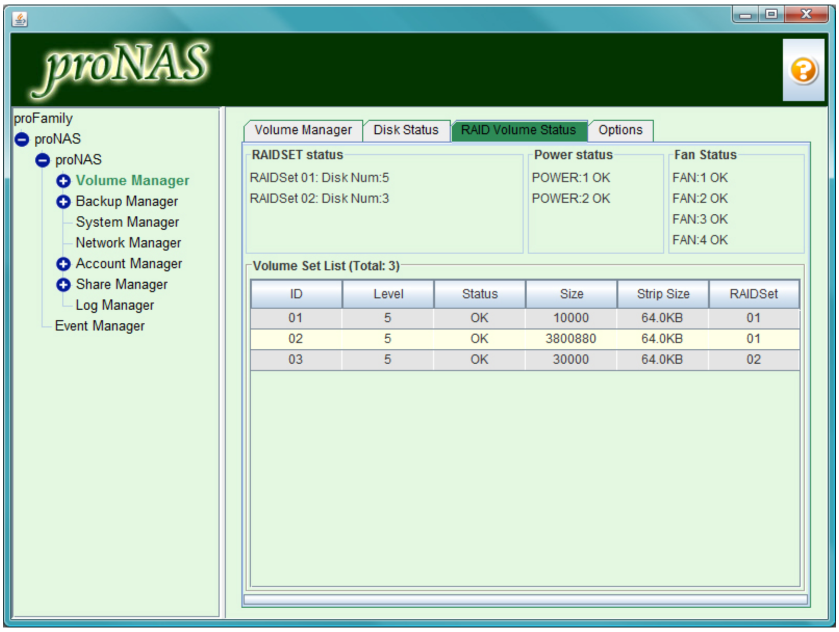
Physical Disk List (Total: 16)

Slot	Status	Temper...	Model	Size	RAIDSet
0-01	Online	29	WDC WD100...	952720	01
0-02	Online	28	WDC WD100...	952720	01
0-03	Online	28	WDC WD100...	952720	01
0-04	Online	26	WDC WD100...	952720	01
0-05	Online	29	WDC WD100...	952720	01
0-06	Online	28	WDC WD100...	952720	Free
0-07	Online	27	WDC WD100...	952720	Free
0-08	Online	24	WDC WD100...	952720	Free
0-09	Online	26	Hitachi HDP7...	475883	02
0-10	Online	26	Hitachi HDP7...	475883	02
0-11	Online	25	Hitachi HDP7...	475883	02
0-12	Empty	24			
0-13	Empty	25			
0-14	Empty	24			
0-15	Empty	24			
0-16	Empty	28			

A “Free” disk can be set as “Hot Spare” disk by selecting the disk and clicking “Set Spare”. A “Hot Spare” disk can be set as “Free” disk by selecting the disk clicking “Remove Spare”.

5.1.6.2 SAS Device Status

The SAS Device Status screen shows the Drive Group or RAID Set status, the power status, the fan status, and the Virtual Drive or Volume Set list, which includes the RAID Level, the size, the stripe size, and the Drive Group or RAID Set where the Virtual Drive or Volume Set was created.



RAIDSET status
RAIDSet 01: Disk Num:5
RAIDSet 02: Disk Num:3

Power status
POWER:1 OK
POWER:2 OK

Fan Status
FAN:1 OK
FAN:2 OK
FAN:3 OK
FAN:4 OK

Volume Set List (Total: 3)

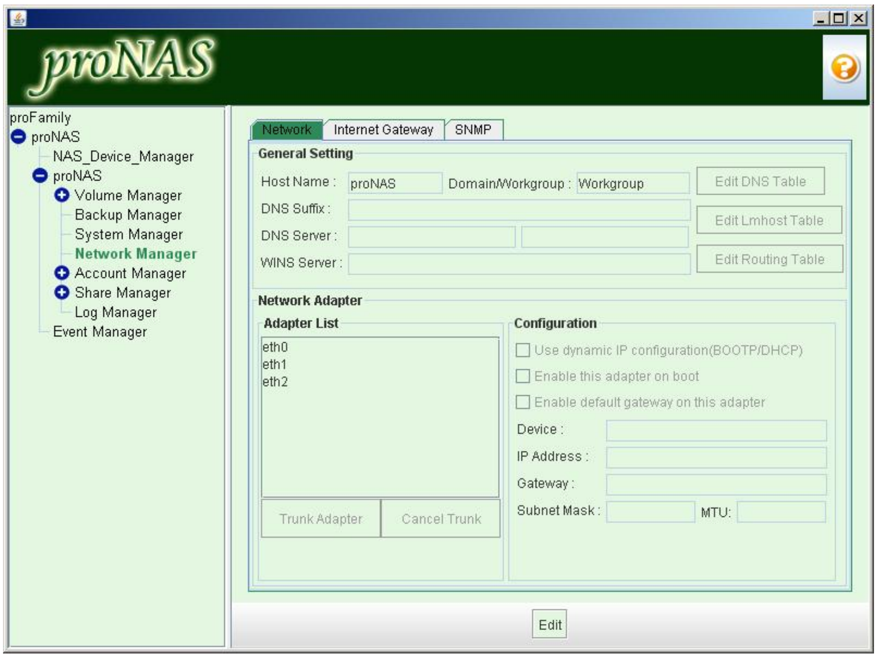
ID	Level	Status	Size	Strip Size	RAIDSet
01	5	OK	10000	64.0KB	01
02	5	OK	3800880	64.0KB	01
03	5	OK	30000	64.0KB	02

5.2 Network Manager

Using the Network Manager, you can configure the NAS network settings. There are three tabs in Network Manager: Network, Internet Gateway, and SNMP.

5.2.1 Network Setting and Trunking

There are two sections in the Network tab, the General Setting section and the Network Adapter section.



General Setting

Host Name : proNAS
Domain/Workgroup : Workgroup
DNS Suffix :
DNS Server :
WINS Server :

Network Adapter

Adapter List

eth0
eth1
eth2

Configuration

□ Use dynamic IP configuration(BOOTP/DHCP)
□ Enable this adapter on boot
□ Enable default gateway on this adapter

Device :
IP Address :
Gateway :
Subnet Mask :
MTU:

The Network tab

Press "Edit" button to configure the Network settings and click "Save" button to update new settings.

General Setting:

- **Host Name -** The NetBIOS name of proNAS, it should be unique.
- **Domain/Workgroup** - Windows domain name or workgroup. Domain name is limited only up to 15 characters. For example: mydomain
- **DNS Suffix** - The DNS suffix appended to server name to complete the server's FQDN. This includes the domain name, for example: mydomain.local
- **DNS Server** - DNS server is responsible for mapping the machine name and IP Address.
- **WINS Server** - WINS Server is responsible for the setting NetBIOS name resolution.

Edit DNS Table: If you have not set the DNS, you can use this button to edit DNS in the DNS table. This is optional.

Edit Lmhost Table: You can use this option to define the resolution of NetBIOS in the Lmhosts table. This is optional.

Edit Routing Table: You can use this option to define routing table. This is optional.

Network Adapter:

The Network Adapter section consists of the Adapter List and the Configuration section. The Adapter List is the list of available Ethernet ports in the system. The number of ports might be two or three depending on different models.

Adapter List: Lists the available Ethernet adapters.

Configuration:

- **Use Dynamic IP Configuration (BOOTP/DHCP) -** If checked, this specifies that this network connection will dynamically obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server or from a Bootstrap Protocol (BOOTP) server.
- **Enable this adapter on boot** – If enabled, this adapter will be active when proNAS starts up.
- **Enable default gateway on this adapter** - If checked, the default gateway will be enabled in this adapter. A default gateway is a local IP router that is used to forward packets to destination beyond the local network. Only one default gateway can be enabled in a certain time.
- **Device** - Displays the type of Network Interface Card.
- **IP address** – Shows the current IP address. To edit IP address, enter the new IP address.
- **Gateway** – Shows the current gateway IP address. To edit, type in a new gateway IP address.
- **Subnet mask** – Shows the current subnet mask setting. To edit, type in the new subnet mask number.
- **MTU** – The MTU size (Maximum Transmission Unit) in bytes. To modify the MTU size for this interface, enter the new MTU size.

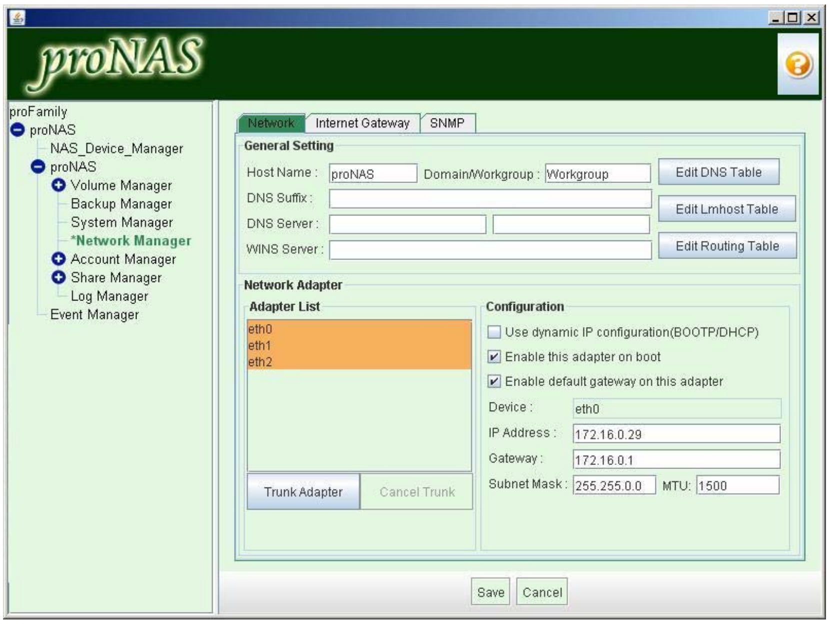
Network Trunking

ProNAS provides the network trunking/bonding function. Ethernet bonding refers to aggregating multiple Ethernet channels together to form a single channel.

NOTE: It is necessary that the network switch supports the type of trunking mode that will be used. Otherwise, the network connections may be unstable.

To create a trunk adapter:

1. Click on the "Edit" button. Press the “Ctrl” key then at the same time select the adapters that will be included in the network trunking then click on "Trunk Adapter" button.



General Setting

Host Name : proNAS Domain/Workgroup : Workgroup

DNS Suffix :

DNS Server :

WINS Server :

Network Adapter

Adapter List

eth0
eth1
eth2

Configuration

□ Use dynamic IP configuration(BOOTP/DHCP)

☑ Enable this adapter on boot

☑ Enable default gateway on this adapter

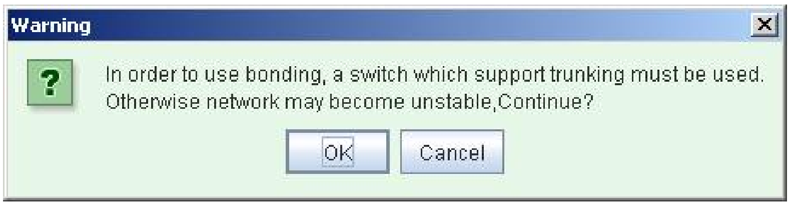
Device : eth0

IP Address : 172.16.0.29

Gateway : 172.16.0.1

Subnet Mask : 255.255.0.0 MTU: 1500

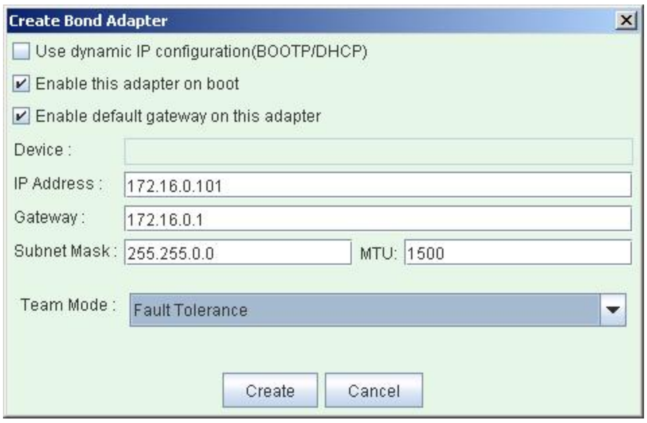
2. A warning message will be displayed. Click “OK” to proceed.



Warning

In order to use bonding, a switch which support trunking must be used. Otherwise network may become unstable,Continue?

3. Setup the network settings. Select the Team Mode to use. Click “Create” when done.



Create Bond Adapter

□ Use dynamic IP configuration(BOOTP/DHCP)

☑ Enable this adapter on boot

☑ Enable default gateway on this adapter

Device :

IP Address : 172.16.0.101

Gateway : 172.16.0.1

Subnet Mask : 255.255.0.0 MTU: 1500

Team Mode : Fault Tolerance

The Team Mode defines the type of operation for the bonded ports.

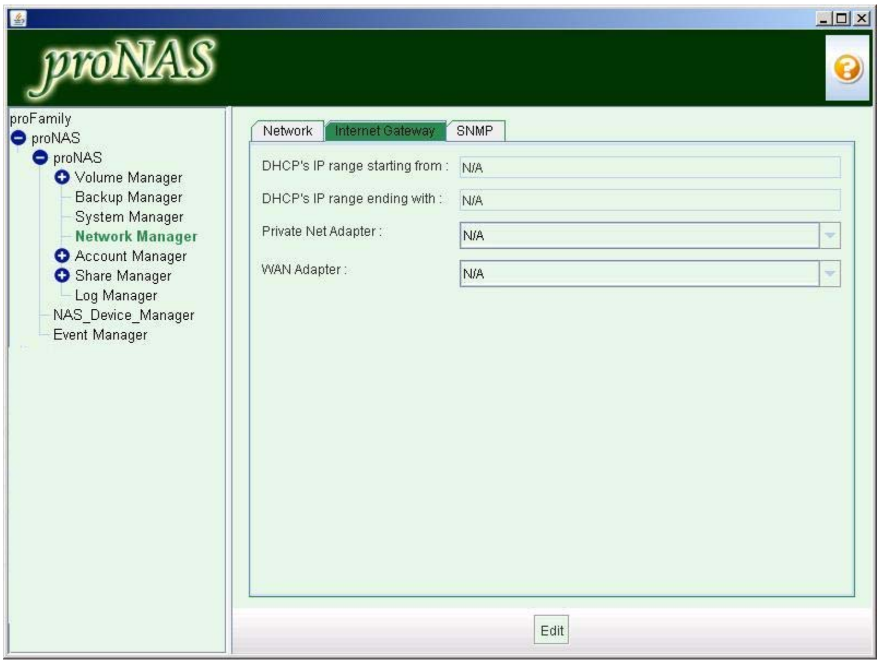
Team Mode options:

- **Fault Tolerant (Active_ Backup)** - Active_Backup policy: If the active Ethernet port fails, the standby Ethernet port will become active. This enhances the availability of access to the NAS.
- **Load balance and Fault Tolerant (XOR)** - XOR policy: Transmit based on source MAC address XOR with destination MAC address. This selects the same slave for each destination MAC address. This mode provides load balance and fault tolerance.
- **Link Aggregation (802.3ad)** - 802.3ad policy: Combines multiple physical network links into a single logical link for increased performance. Transmits and receives on all slaves in the active aggregator. Pre-requisite: the network switch must support IEEE 802.3ad.
- **Load Balance (ALB)** - ALB (Adaptive load balancing) policy: The receive load balancing is achieved by ARP negotiation and does not require special switch support.

4. Connect to proNAS using the new IP address used in network trunking.

5.2.2 Internet Gateway

proNAS provides Internet gateway function which enables proNAS to act as an Internet Gateway, integrating DHCP service, routing and NAT. Using Internet gateway function, administrators can easily enable and disable the Internet access for network users.



DHCP's IP range starting from : N/A

DHCP's IP range ending with : N/A

Private Net Adapter : N/A

WAN Adapter : N/A

To configure Internet Gateway, press “Edit” button.

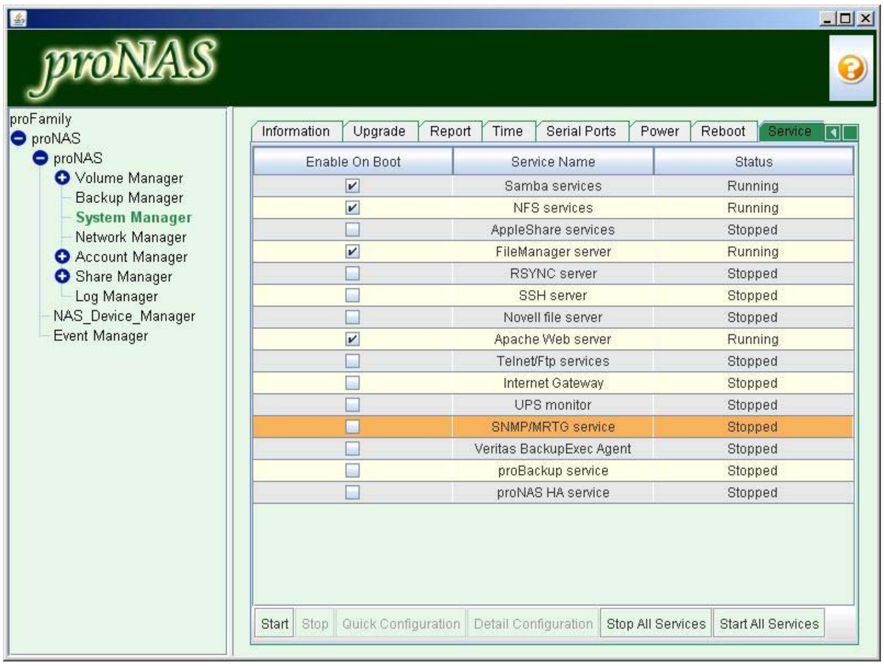
Configuration options:

- **DHCP's IP range starting from -** means the lower bound (starting) range of private IP addresses for DHCP
- **DHCP's IP range ending with -** means the upper bound (ending) range of private IP addresses for DHCP
- **Private Net Adapter -** means the port connected to private network. This port has to be a Static port and could also be a Trunk port.
- **WAN Adapter**: means the port connected to WAN or Internet. This port could be a Trunk port.

NOTE: When using Internet Gateway function, make sure the Internet Gateway service is enabled in the Service tab of System Manager.

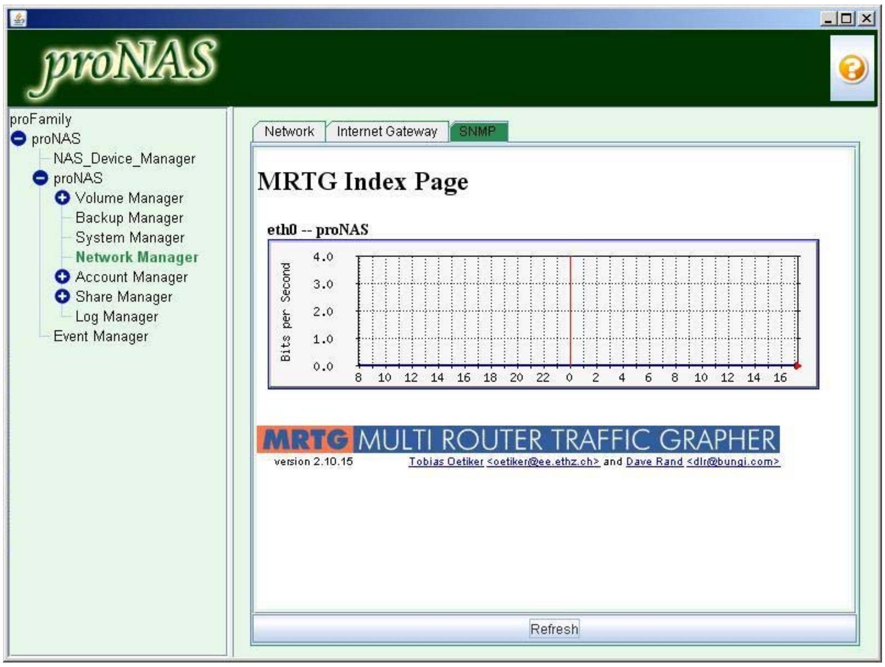
5.2.3 SNMP/MRTG

The SNMP/MRTG service can be enabled to monitor proNAS network traffic. Select Service tab of System Manager then enable SNMP/MRTG service. Click “Start” to enable the service.



Enable On Boot	Service Name	Status
☑	Samba services	Running
☑	NFS services	Running
□	AppleShare services	Stopped
☑	FileManager server	Running
□	RSYNC server	Stopped
□	SSH server	Stopped
□	Novell file server	Stopped
☑	Apache Web server	Running
□	Telnet/Ftp services	Stopped
□	Internet Gateway	Stopped
□	UPS monitor	Stopped
□	SNMP/MRTG service	Stopped
□	Veritas BackupExec Agent	Stopped
□	proBackup service	Stopped
□	proNAS HA service	Stopped

To view the SNMP/MRTG network traffic information, select the SNMP tab in Network Manager.



MRTG Index Page

eth0 -- proNAS

version 2.10.15 Tobias Oetiker <oetiker@ee.ethz.ch> and Dave Rand <dlr@bungi.com>

For more information about MRTG service, please visit http://www.mrtg.org.

5.3 Account Manager

With Account Manager, the administrator can manage and administer local accounts as well as import external domain accounts. proNAS will utilize external directory services to do account authentications which currently supports ADS/PDC and NIS.

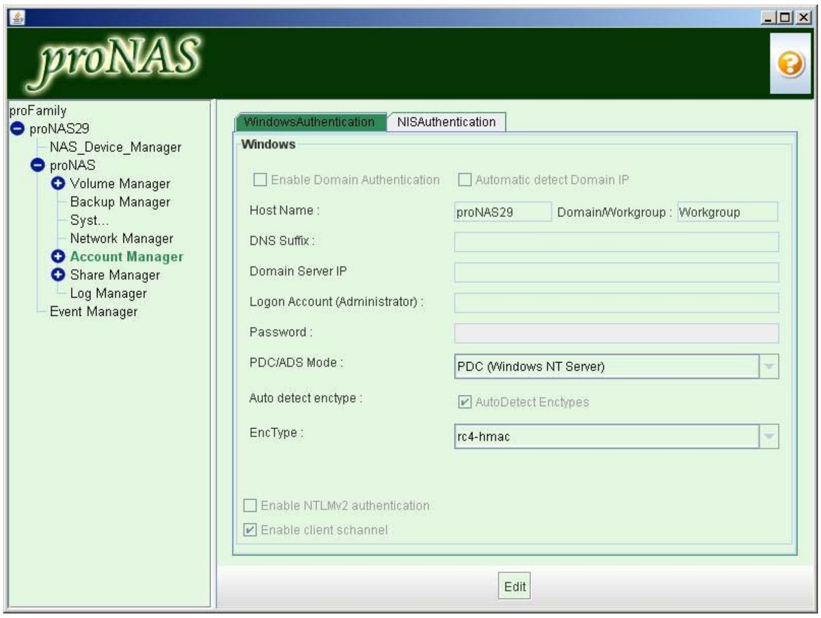
The main functions of the Account Manager are:

- Authentication
- User Account
- Group Management

5.3.1 External Accounts Integration (Joining Windows or NIS Domain)

You can utilize external directory services to authenticate accounts. Currently, PDC/ADS and NIS authentication are supported. You may choose any one of them or both at the same time depending on your network environment.

5.3.1.1 Windows Authentication



□ Enable Domain Authentication □ Automatic detect Domain IP

Host Name : proNAS29 Domain/Workgroup : Workgroup

DNS Suffix :

Domain Server IP

Logon Account (Administrator) :

Password :

PDC/ADS Mode : PDC (Windows NT Server)

Auto detect enctype : ☑ AutoDetect Enctypes

EncType : rc4-hmac

□ Enable NTLMv2 authentication

☑ Enable client schannel

If you would like to integrate proNAS with Windows environment, please select “Edit” button then check "Enable Domain authentication". Set the necessary Windows options then click “Save” to update settings.

NOTE: Hostname, Domain name and DNS Suffix need to be set first in Network Manager.

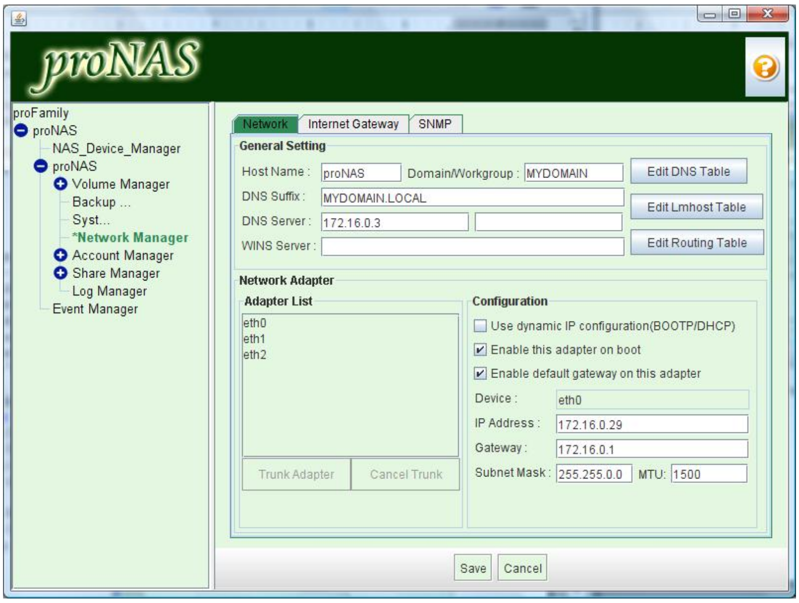
Windows options:

- **Automatic detect Domain IP** – This is enabled by default. When enabled, proNAS will try to automatically detect the domain server's IP address.
- **Hostname** - Indicates the NetBIOS name of proNAS; must be set in Network Manager.
- **Domain/Workgroup** - Windows Domain name; must be specified in Network Manager.
- **DNS Suffix** - The DNS suffix used; must be set in Network Manager.
- **Domain Server IP** - The IP address of the domain server. proNAS will automatically acquire the domain server's IP address after setting the Domain name in Network Manager if "Automatic detect Domain IP" option is enabled. When "Automatic detect Domain IP" option is disabled, you need to manually enter the domain server's IP address.
- **Logon account (Administrator)** – the administrator's logon name in the Domain Controller
- **Password** - the administrator's password in the Domain Controller.
- **PDC/ADS Mode** – The type of Domain Controller. Choose PDC for Windows NT Server or ADS for Windows 2000/2003/2008 Server.
- **Auto Detect Enctypes –** This option automatically detects the encryption type used in Windows authentication. To manually select the encryption type, disable this option and select the preferred encryption type from the EncType drop-down list.
- **Enable NTLMv2 authentication** - This parameter determines whether or not smbclient will attempt to authenticate itself using the NTLMv2 encrypted password. If enable, proNAS will only sent NTLMv2 and LMv2 responses. NTLMv2 authentication protocol is available only on WindowsNT4 with SP4 and Windows 2000 or later. Default is disabled.
- **Enable client schannel** - This controls whether the client offers or even demands the use of the netlogon schannel. Default is auto, means it offers the schannel but does not enforce it.

5.3.1.2 Sample Steps to Join the NAS to Windows AD Domain:

1. Select Network Manager. In Network Manager –> Network tab, click "Edit" to configure network settings.
2. Change the default proNAS Host Name if there are other proNAS systems in the network. Enter the Windows Domain name in "Domain/Workgroup". For example: MYDOMAIN

3. Enter the DNS Suffix. The DNS suffix is the name appended to the server name to complete the server's FQDN. This includes the domain name. For example: MYDOMAIN.LOCAL
4. Enter the DNS Server and WINS Server (IP address) as necessary.
5. Click "Save" to update changes.



General Setting

Host Name : proNAS   Domain/Workgroup : MYDOMAIN

DNS Suffix : MYDOMAIN.LOCAL

DNS Server : 172.16.0.3

WINS Server :

Network Adapter

Adapter List: eth0, eth1, eth2

Configuration

□ Use dynamic IP configuration(BOOTP/DHCP)

☑ Enable this adapter on boot

☑ Enable default gateway on this adapter

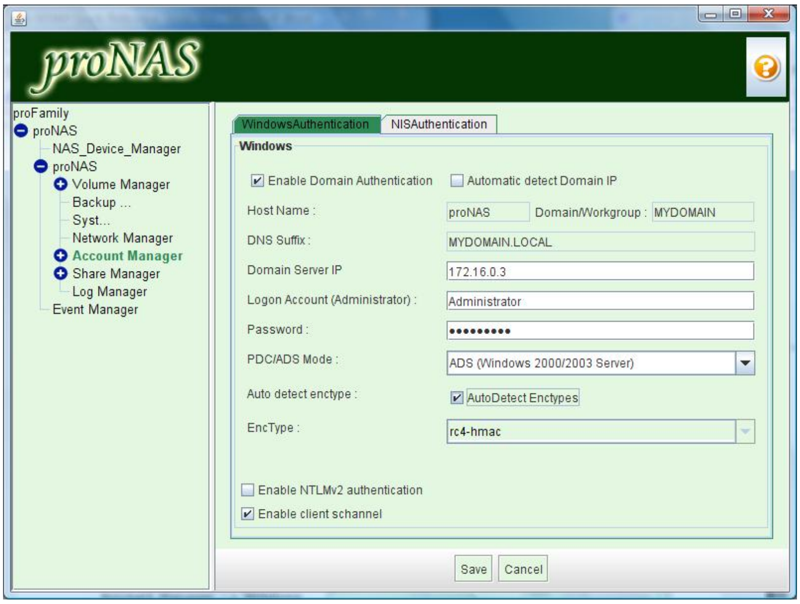
Device : eth0

IP Address : 172.16.0.29

Gateway : 172.16.0.1

Subnet Mask : 255.255.0.0   MTU: 1500

6. Select Account Manager. In Account Manager –> Windows Authentication, click "Edit".
7. Tick "Enable Domain Authentication" option.
8. If the Domain Server IP is not detected (not shown), you can manually specify the Domain Server IP by removing the check mark in "Automatic Detect Domain IP" and entering the Domain Server IP address.
9. Enter the Domain Administrator Account and Password.
   NOTE: No need to include "domain-name\" in Domain Administrator Account.
10. Select the Domain Server mode (PDC or ADS).
11. If needed, change the encryption type to the same type used by your domain server.
12. Click "Save". The NAS will be joined to Windows Domain in a while.



Windows

☑ Enable Domain Authentication   □ Automatic detect Domain IP

Host Name : proNAS   Domain/Workgroup : MYDOMAIN

DNS Suffix : MYDOMAIN.LOCAL

Domain Server IP : 172.16.0.3

Logon Account (Administrator) : Administrator

Password : •••••••••

PDC/ADS Mode : ADS (Windows 2000/2003 Server)

Auto detect enctype : ☑ AutoDetect Enctypes

EncType : rc4-hmac

□ Enable NTLMv2 authentication

☑ Enable client schannel

13. To verify, select Account under Account Manager; the user accounts should be shown. You can also verify group accounts in Group List.

5.3.1.3 NIS Authentication

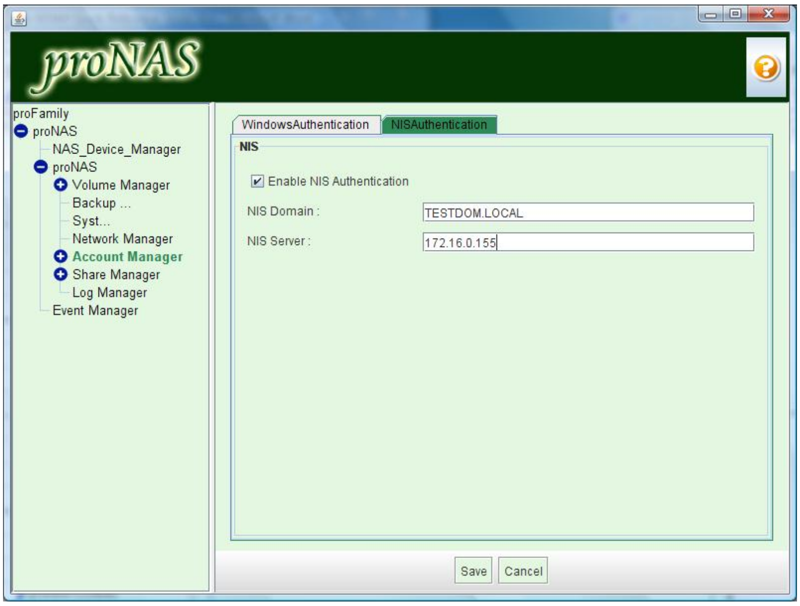
If you would like to integrate proNAS with UNIX/Linux environment, please select “NIS Authentication” tab and click “Edit” button then check "Enable NIS authentication". Set the necessary configuration options then click “Save” to update settings.

Configuration Options:

- **NIS Domain** - Enter the NIS domain name
- **NIS server** - Enter the IP Address of NIS server.

5.3.1.4 Sample Steps to Join NIS Domain:

1. Under Account Manager, select NIS Authentication tab. Click Edit.
2. Check the Enable NIS Authentication option. Enter the NIS Domain name (e.g.: TESTDOM.LOCAL) and NIS Server IP address or FQDN. Click Save when done.
3. Click Account under Account Manager to verify that the NIS Accounts are listed in the Account List, or select Group to display the NIS Groups in the Group List.



☑ Enable NIS Authentication

NIS Domain : TESTDOM.LOCAL

NIS Server : 172.16.0.155

5.3.2 Local Account and Group Management

Account Management

The Account List in Account Manager includes Local users and External users, ADS/PDC or NIS.

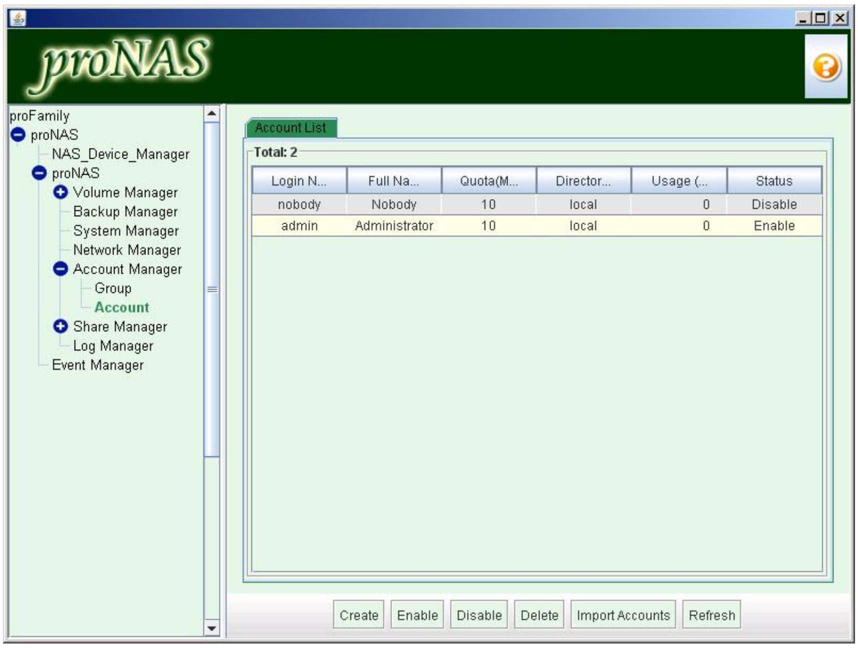
In Account menu, admin can perform the following functions:

- Create a new Local Account
- Enable and Disable an Account
- Modify and Delete an Account
- Mass Import Accounts
- Refresh the Account List

Creating a new Local account

Following are the steps to create a new Local account:

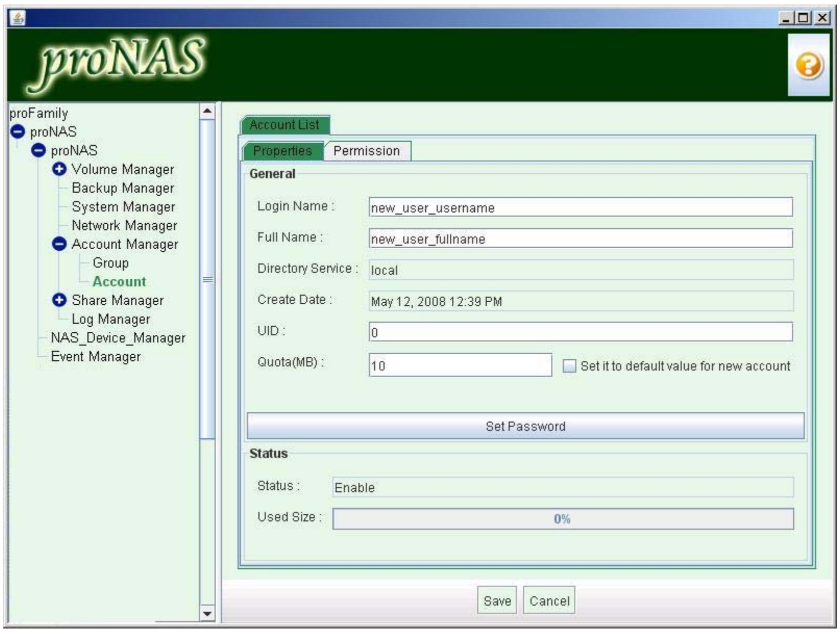
1. Select Account Manager in the proFamily tree. Choose Account node under the Account Manager. It will display all accounts under the Account List tab.



Total: 2

Login N...	Full Na...	Quota(M...	Director...	Usage (...	Status
nobody	Nobody	10	local	0	Disable
admin	Administrator	10	local	0	Enable

2. Press the "Create" button. System will display "Account List tab". Account List tab consist of two tabs, "Properties" and "Permission". In the Properties tab, enter the necessary information.



General

Login Name : new_user_username

Full Name : new_user_fullname

Directory Service : local

Create Date : May 12, 2008 12:39 PM

UID : 0

Quota(MB) : 10 □ Set it to default value for new account

Status

Status : Enable

Used Size : 0%

General:

- **Login Name** - Input the login name, it should be unique in proNAS
- **Full Name -** the complete name of the account
- **Directory Service -** system will display if the directory service is Local or ADS/PDC,NIS
- **Create Date -** system will display the create date of the account.
- **UID -** In UNIX or Linux, OS will assign a unique user number called UID to access the system resource. (UID range is 1 to 65535). proNAS may either assign a new UID automatically starting from 500 or you can manually specify the UID. Domain accounts will have a UID starting from 10000-30000.
- **Quota Size (MB)** - This specifies the quota (usable space) of a user for its home folder. The default is 10MB.
- **Set it to default value for new account** – When this option is enabled and the Quota Size value has been changed from 10MB to another value, the new value set in Quota Size will become the new default Quota Size when other accounts are created.
- **Set Password** – Click this button to set the account's password. Passwords have to be at least 6 characters.

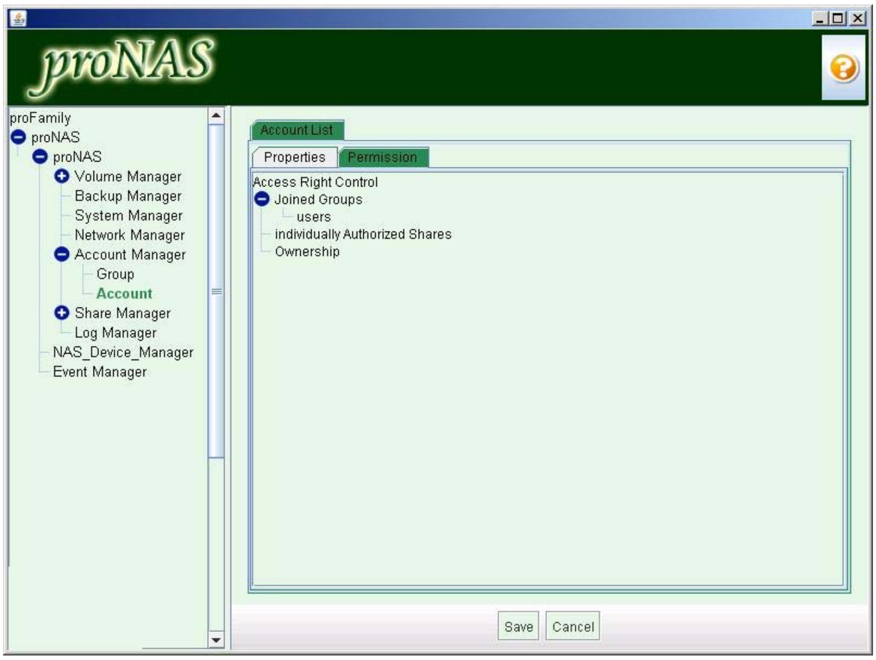
Status:

- **Current status:** Displays Enable or Disable.
- **Used Size (MB):** Displays the current used size.

Use the following guidelines to ensure that you are using a valid Account name:

- Account names must start with a small alphabet letter.
- Account names cannot be longer than 32 characters.
- Account names should be unique. No account names must be the same. No account names must be the same with share names.
- Account names cannot contain blank spaces.
- Account names cannot begin with a dash (-) and cannot consist of only a single dash.
- Account names cannot contain the following characters: /\[]";:|<>+=,?*
- Account names cannot be duplicated with the system default accounts, i.e. root, mail, news, operator, gopher, nobody, ftp, games, rpc, adm, nobody, etc.

3. After completing the settings, press the "Save" button to save settings, or you may go to "Permission" tab to have a look at the permissions of the account then click “Save” button when done.



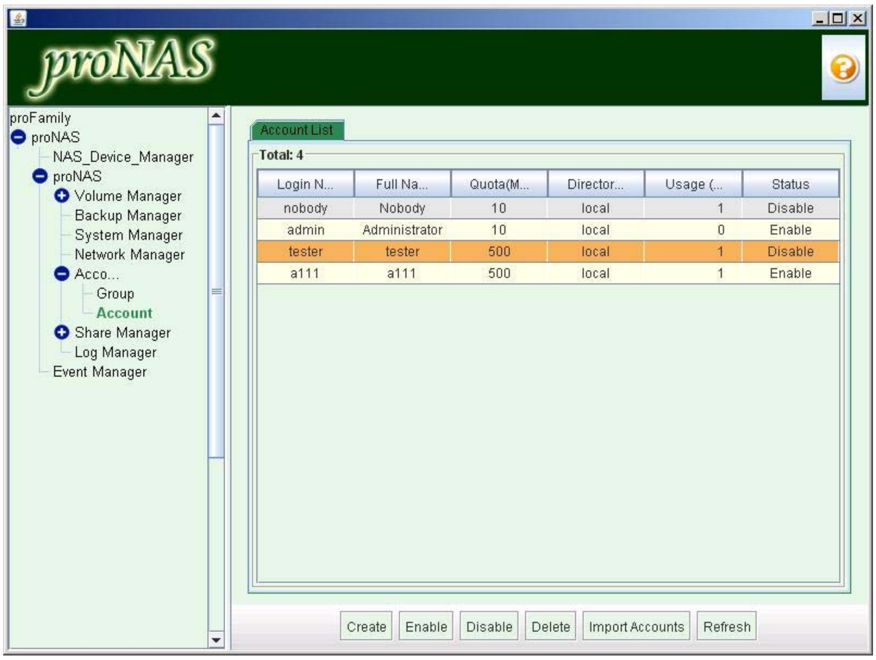
Permission tab

- **Joined Groups:** The account has gained access right because of joining certain groups.
- **Individually Authorized Shares:** Implies that the account has gained access rights individually.
- **Ownership:** Implies that the account has gained access right because it is the owner.

NOTE: Newly created accounts will automatically be a member of "users" group.

Enabling and Disabling an Account

Account Manager allows the administrator to enable or disable a user account. When an account is disabled, the account cannot be used to login and access proNAS.
To forbid certain user account in accessing proNAS, highlight the account then press "Disable" button. The account will be shown with "Status" as Disable. If you would like to re-enable the user account proNAS, press "Enable" button. Disabling account "admin" is not allowed as well as all ADS/PDC and NIS accounts.



Total: 4

Login N...	Full Na...	Quota(M...	Director...	Usage (...	Status
nobody	Nobody	10	local	1	Disable
admin	Administrator	10	local	0	Enable
tester	tester	500	local	1	Disable
a111	a111	500	local	1	Enable

Deleting an Account

If you would like to delete a certain account, highlight the account then press "Delete" button. The user's home directory will be deleted. If the user owns one of the share, the owner of that share will be set to "admin". Account "admin" is not allowed to be deleted as well as ADS/PDC and NIS accounts.

Modifying an Account

If you want to modify an account, double-click on the account. You can only modify the password and permissions. If the account is an external domain account (created by ADS/PDC or NIS domain server), the account and password can not be modified in proNAS Account Manager. In such a case, you can only modify the permissions.

Importing of Accounts

proNAS provides Import Account function for creating large number of accounts instead of adding an account one by one. Administrator can create multiple user accounts in a text file with the following format: UID, Logon Account, Logon Password, Full Name. Example:

```
1019, david, proware, David Huang
1020, rocky, proware, Rocky Lee
```

To import the accounts, click on "Import Accounts" button then select the text file.

NOTE: The information for each account must start on a new line. If account creation fails for any account, proNAS skips that line (of account information) and continues with the next line.

Refreshing the Account List

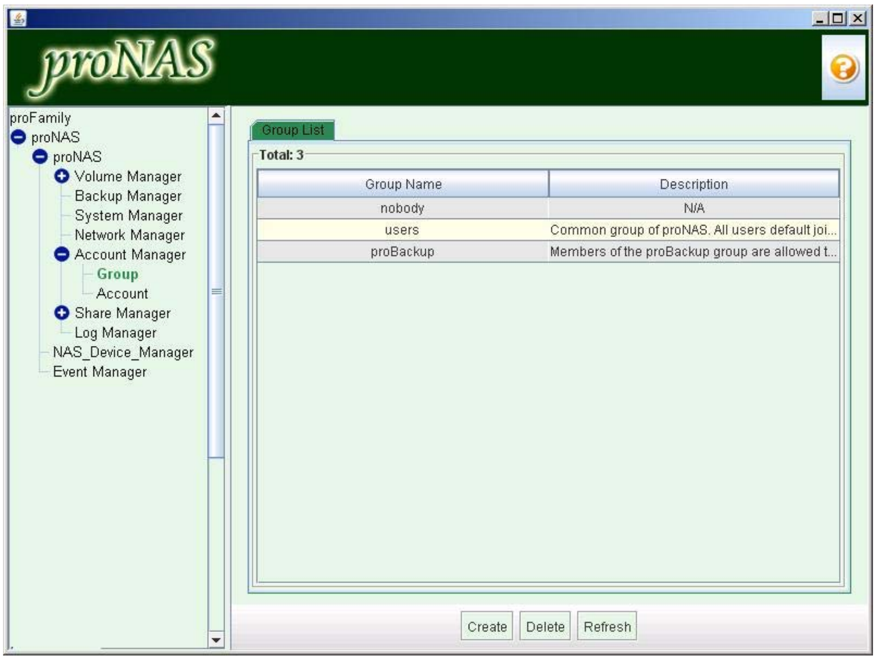
Use the “Refresh” button to automatically synchronize any new accounts created in ADS/PDC or NIS domain.

Group Management

Using group management, admin can organize access to proNAS shares. For example, a Sales group can be created for the sales department and this group can be assigned read-write access to the Sales Report share. All account members of the Sales group can have access to the Sales Report share.

Group List tab

The Group List tab shows the Local and External (ADS/PDC or NIS) Groups.



Total: 3

Group Name	Description
nobody	N/A
users	Common group of proNAS. All users default joi...
proBackup	Members of the proBackup group are allowed t...

Group management allows the administrator to:

- Create or Delete a Local group
- Modify a Group
- Refresh the Group List

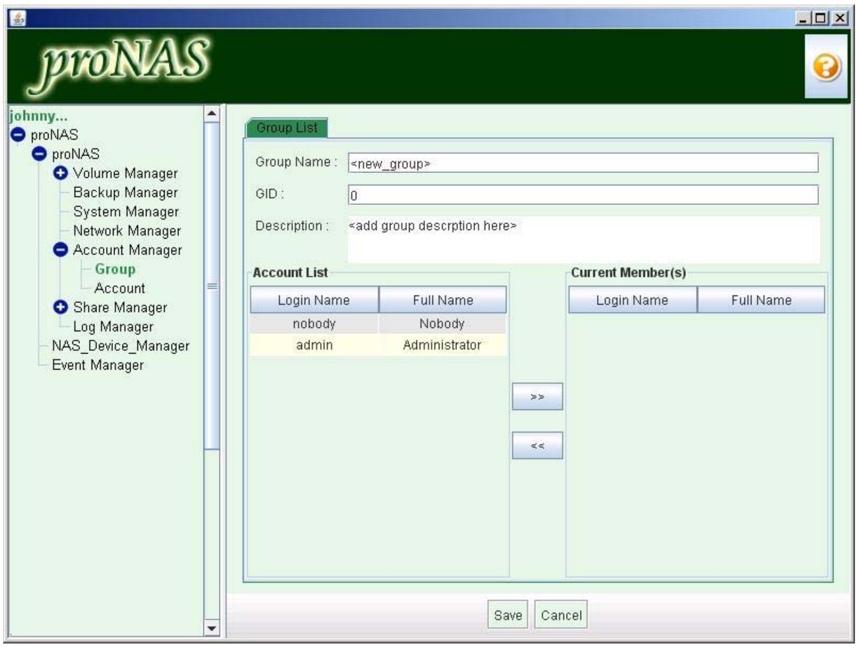
proNAS has two default groups, "users" and "proBackup". Every local user that will be created will automatically become a member of users group. proBackup group is used by proNAS for the proBackup service.

Creating a new Local Group

When a Local Group is added, it is created in the local account database of NAS. One account can become a member of more than one group.

Following are the steps to create a new Local Group:

1. Select Account Manager in the proFamily tree. Choose Group node under the Account Manager. It will display all groups under the Group List tab. Press the "Create" button.
2. Enter the necessary information. Refer to options below.



Group Name : <new_group>

GID : 0

Description : <add group descrption here>

Account List

Login Name	Full Name
nobody	Nobody
admin	Administrator

Current Member(s)

Login Name	Full Name

Create Group Options:

- **Group Name** - Enter the name of new group. It should be unique.
- **GID** - Group ID. proNAS will either automatically assign a GID when you create a group, or you can manually specify a GID.
- **Description** – Additional information or description about the Group can be entered here.

Account List – shows the list if accounts that are available and can be joined to the group

Current Member(s) – shows the list if accounts that are currently member of the group

Use the following guidelines to ensure that you are using a valid Group name:

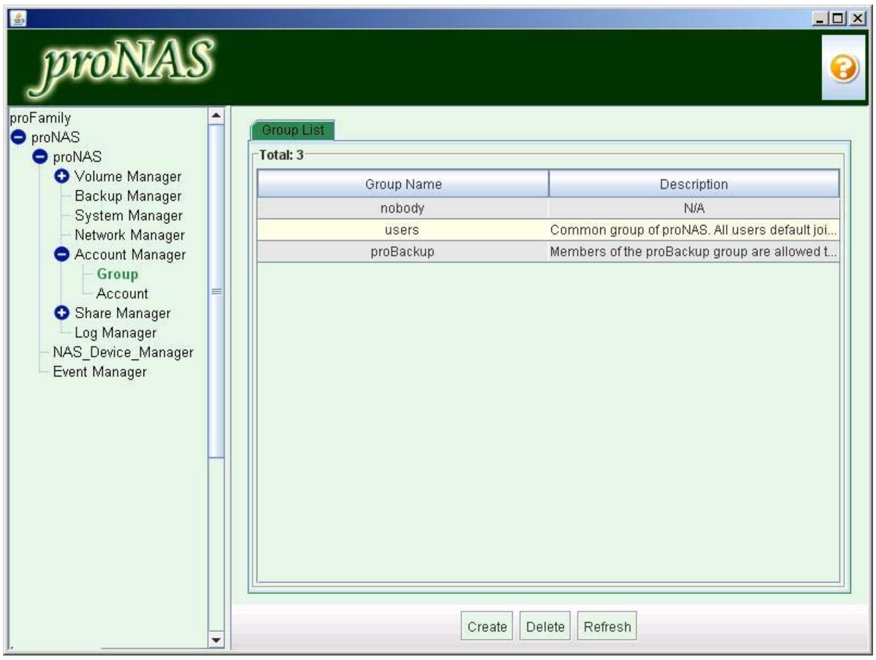
- Group names cannot be longer than 16 characters.
- Group names should be unique. No group names must be the same.
- Group names cannot contain blank spaces.
- Group names cannot begin with a dash (-) and cannot consist of only a single dash.
- Group names cannot contain the following characters: /\[]";:|<>+=,?*

- ♦ Group names cannot be duplicated with the system default groups, i.e. root, mail, news, operator, gopher, nobody, ftp, games, rpc, adm, nobody, etc.

3. In the Account List, select the account(s) that will be joined to the group then click the ">>" button. The accounts will appear in the Current Member(s) list. To remove an account from the group, select the account in Current Member(s) list then click "<<" button.
4. Click "Save" button to save settings.

Deleting a Local Group

To delete a group, select the group to be deleted and then click the "Delete" button. ADS/PDC and NIS groups are not allowed to be deleted. Default group "users" and "proBackup" cannot also be deleted.



Total: 3

Group Name	Description
nobody	N/A
users	Common group of proNAS. All users default joi...
proBackup	Members of the proBackup group are allowed t...

Modifying a Group

To modify a group, double click the group in Group List tab. The "Group List" tab will be displayed in edit mode. Group name, description, group members are allowed to be modified however this is only applicable to local groups. ADS/PDC and NIS groups are not allowed to be modified. Default group "users" and "proBackup" cannot be modified. ADS/PDC and NIS domain accounts are also not allowed to be joined to any local group except to "proBackup" group.

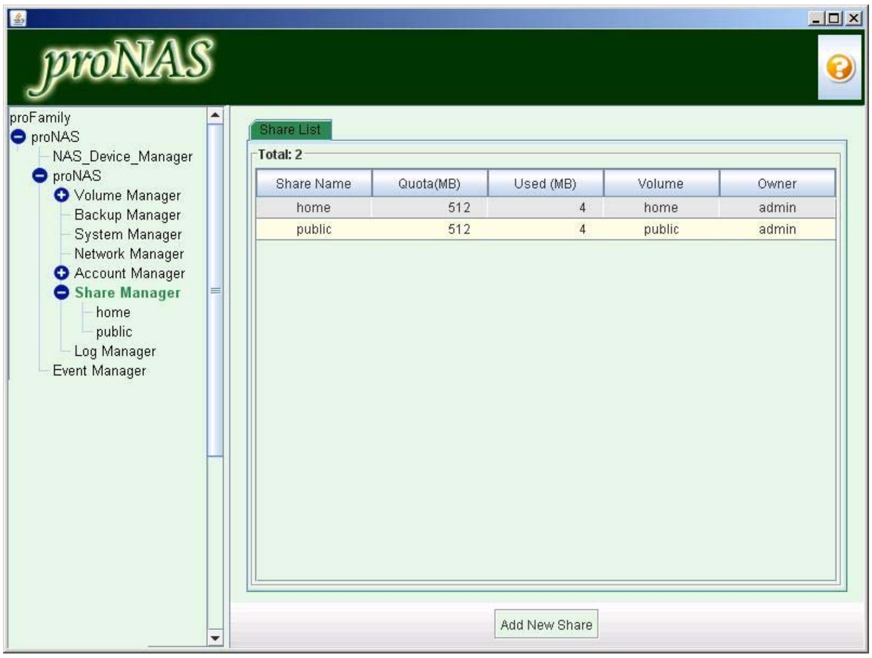
Refreshing the Group List

Use the "Refresh" button to automatically synchronize any new groups created in ADS/PDC or NIS domain.

5.4 Share Manager

In proNAS Share Manager, you can create and configure a Share, assign a share owner, assign user permission, and specify file sharing protocol. Under this node you can also use duplication function and rsync utility. Duplication is a share function in which you can replicate your share into another share using file level replication. Rsync utility is used to copy files either to or from a remote host, or locally on the current host.

In the "Share List" tab, you can list the current shares and also display share information such as share name, quota, used space, logical volume and share owner. There are 2 Default Share in proNAS: "home" and "public".



Total: 2

Share Name	Quota(MB)	Used (MB)	Volume	Owner
home	512	4	home	admin
public	512	4	public	admin

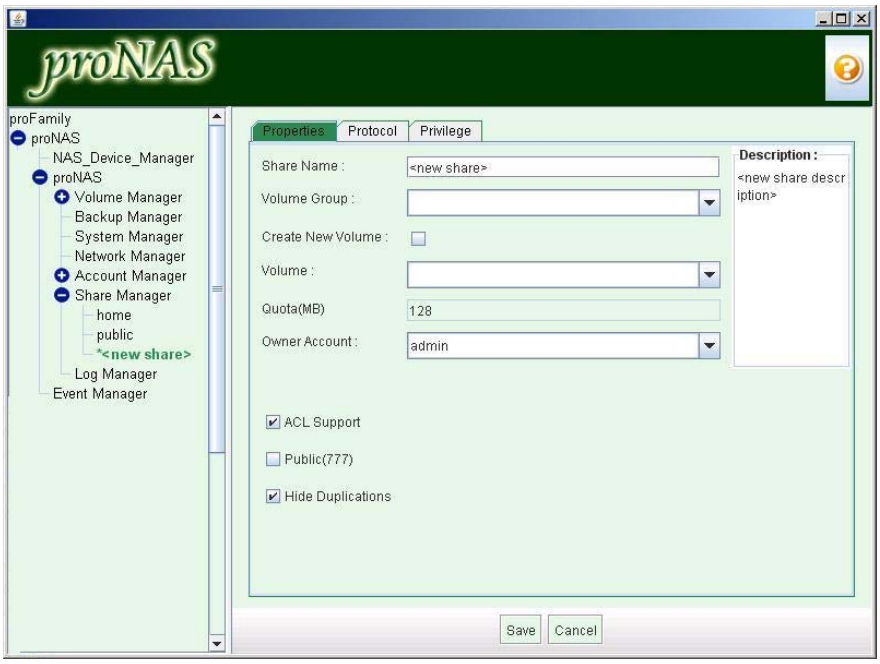
Share folder gets created under a logical volume. Make sure that an LV is already created before creating the share folder or admin can create the share folder and LV simultaneously, which can be done using the option “Create New Volume” in Properties tab of Share Manager.

5.4.1 Share Management

5.4.1.1 Creating a New Share

To create a new share folder:

1. Select Share Manager then press "Add New Share" button.
2. Configure all necessary share options in Properties, Protocol, and Privilege tabs.
3. Click “Save” button to save share settings.



Share Name : <new share>

Volume Group :

Create New Volume : □

Volume :

Quota(MB) 128

Owner Account : admin

Description : <new share description>

☑ ACL Support

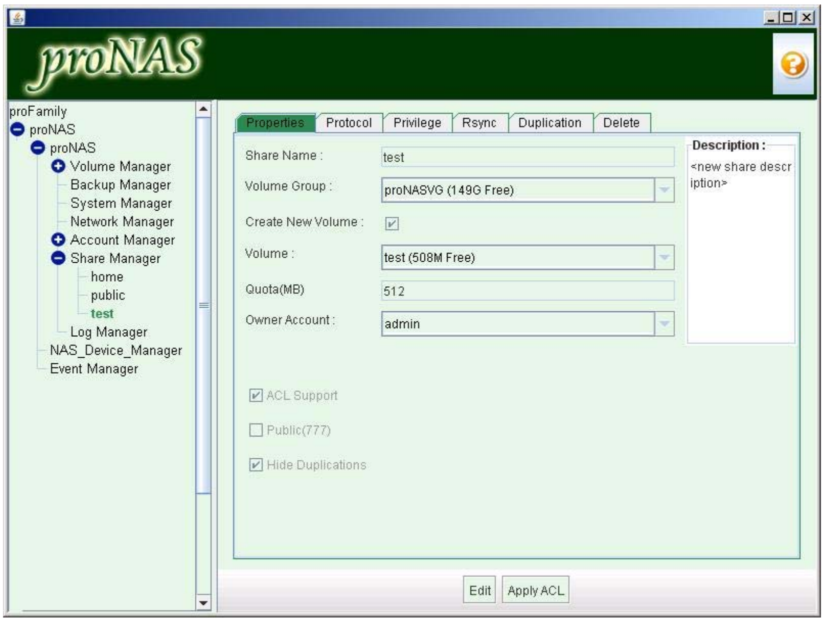
□ Public(777)

☑ Hide Duplications

NOTE: After creating the share and setting the Properties, Protocol and Privilege tabs, you can go back to these tabs and modify the various options. To edit, click the share name in Share Manager and click “Edit” button.

5.4.1.2 Applying ACL

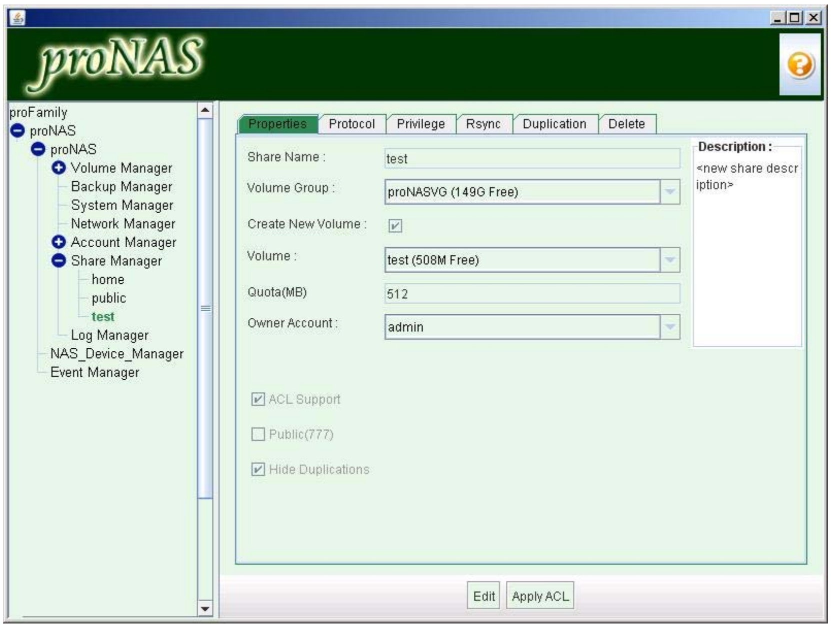
When applying ACL in a share, all the files and subfolders under this share will inherit the share's permission. "Apply ACL" will propagate the ACL settings of the share folder into all of its child directories and files. For example, if user1 has read/write permission on the sub-folder but read only on the share, after applying ACL, user1 will now have a read-only permission on the sub-folder.



Share Name : test
Volume Group : proNASVG (149G Free)
Create New Volume : ☑
Volume : test (508M Free)
Quota(MB) 512
Owner Account : admin
Description : <new share description>
☑ ACL Support
□ Public(777)
☑ Hide Duplications

5.4.1.3 Modifying a Share

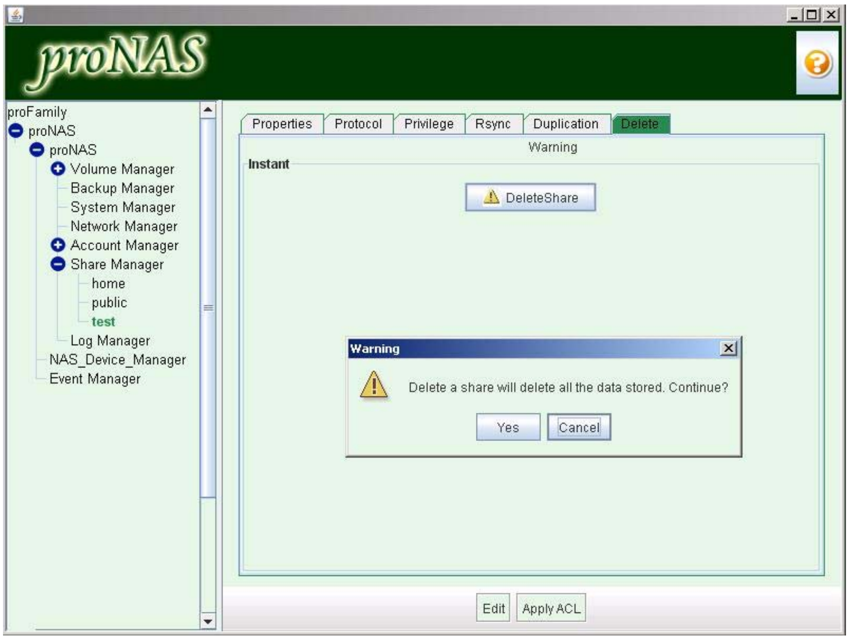
After creating the share, you can modify the Properties, Protocol, and Privilege tabs, as well as setup the Rsync and Duplication functions. Click the “Edit” button to modify the share.



Share Name : test
Volume Group : proNASVG (149G Free)
Create New Volume : ☑
Volume : test (508M Free)
Quota(MB) 512
Owner Account : admin
Description : <new share description>
☑ ACL Support
□ Public(777)
☑ Hide Duplications

5.4.1.4 Deleting a Share

If you delete a share, all the data in the share is deleted. If the data in the share is no longer needed or a backup of the data has been made, you may delete a share. If there is no data backup, we recommend you to create a backup first before deleting a share.



Warning

Delete a share will delete all the data stored. Continue?

5.4.2 Properties Setting

The Properties tab contains the following settings:

- **Share Name -** Input the share name, it should be unique in proNAS.

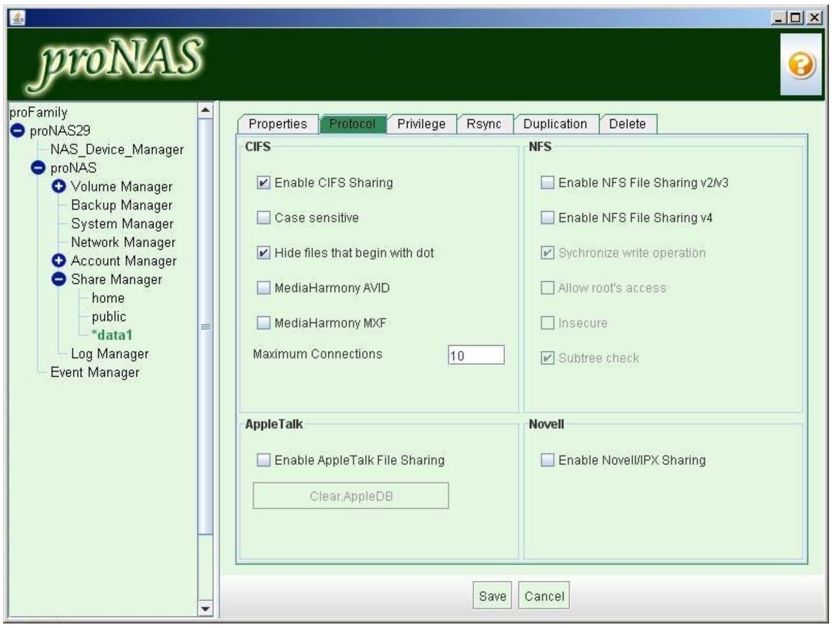
  Use the following guidelines to ensure that you are using a valid Share name:

  - Names cannot be longer than 31 characters.
  - Names should be unique. It cannot be a duplicate with other LV names, shares, and Account names.
  - Names cannot contain blank spaces.
  - Names cannot begin with a dash (-) and cannot consist of only a single dash.
  - Names cannot contain the following characters: /\[]";:|<>+=,?*

- **Volume Group (VG)** - Choose a volume group from the list. Only Volume groups that has member disk will be displayed. System will also display the available space of the volume group.
- **Create New Volume (LV)** -If you check this option, system will create LV as well as create the new Share. The LV name will be the same as the share name.
- **Volume -** Select a logical volume from the selected volume group.
- **Quota (MB) -** Input the size of the share. This is also the size of the logical volume to be created if you choose to create a volume at the same time.
- **Owner Account -** Specifies the owner of the share.
- **ACL Support** – Specifies if the share will support ACL permission (option is enabled by default) or support “chmod” permission.
- **Public (777)** - This option allows you to set a share as a public share. When enabled, any user within the specified private net can connect to this share.
- **Hide Duplications** - This option allows you hide or unhide the "_Duplication" folder in this share. The default will be hidden.

5.4.3 Protocol Setting

proNAS supports the following share protocols: CIFS, NFS, AppleTalk, and Novell, which can be set in Protocol tab when creating the share or when in edit mode.



CIFS

☑ Enable CIFS Sharing

☐ Case sensitive

☑ Hide files that begin with dot

☐ MediaHarmony AVID

☐ MediaHarmony MXF

Maximum Connections 10

NFS

☐ Enable NFS File Sharing v2/v3

☐ Enable NFS File Sharing v4

☑ Sychronize write operation

☐ Allow root's access

☐ Insecure

☑ Subtree check

AppleTalk

☐ Enable AppleTalk File Sharing

Novell

☐ Enable Novell/IPX Sharing

5.4.3.1 CIFS

- **Enable CIFS Sharing** - This specifies whether to enable or disable CIFS sharing
- **Case sensitive** - This control whether filenames are case sensitive.
- **Hide files that begins with dot** - This option controls whether files starting with a dot will appear as hidden files.
- **MediaHarmony AVID** – This option enables media file interoperability for non-linear editors. It allows multiple editing clients (Avid editors) to interoperate without conflicts.
- **MediaHarmony MXF** – This option enables media file interoperability for non-linear editors. It allows on-the-fly unwrapping of MXF-wrapped DV essence so that a Final Cut Pro client can share the same DV media files as an Avid client.
- **Maximum connection** - This option limits the number of simultaneous connections at a certain time. A value of zero means an unlimited number of connections will be possible in this share.

NOTE: Only one option from "MediaHarmony AVID" and "MediaHarmony MXF" can be enabled or selected at a time.

NOTE: The default setting of "Maximum Connections" is 10. If there will be more than 10 client connections via CIFS simultaneously, change the setting to a higher value. For unlimited number of simultaneous connections, set it to zero (0).

5.4.3.2 NFS

- **Enable NFS file sharing v2/v3** - This specifies whether to enable or disable NFS version 2 / version 3 file sharing
- **Enable NFS file sharing v4** - This specifies whether to enable or disable NFS version 2 / version 3 file sharing
- **Synchronize write operation** – Use this option to enable or disable write caching
- **Allow root's access** – Use this option to allow or disallow access by root super user account
- **Insecure** - If you choose this option, it means only the port under 1024 can access, it provides higher security
- **Subtree check** – Use this option to enable or disable subtree checking. A subtree check happens if a subdirectory of a filesystem is exported, but the whole filesystem isn't then whenever a NFS request arrives, the server must check not only that the accessed file is in the appropriate filesystem (which is easy) but also that it is in the exported tree (which is harder).

5.4.3.3 AppleTalk

Enable AppleTalk File Sharing: This specifies whether to enable or disable AppleTalk file sharing.

5.4.3.4 Novell

Enable Novell/IPX Sharing: This specifies whether to enable or disable Novell Netware file sharing.

Accessing proNAS shares under Linux

For NFS share:

Usage: mount -t nfs x.x.x.x:/mnt/proNAS/volume/share /mnt/temp

where:

x.x.x.x = proNAS IP address

/mnt/proNAS/volume/share = the complete path of the NFS share. You may use the command "showmount -e x.x.x.x" to query the complete path.

/mnt/temp = local mount point on the client

For CIFS share:

Usage: mount -t smbfs //x.x.x.x/share /mnt/temp -o username=account,password=secret

or

mount.cifs //x.x.x.x/share /mnt/temp -o username=account,password=secret

or

smbmount //x.x.x.x/share /mnt/temp -o username=account,password=secret

where:

x.x.x.x = proNAS IP address

share = CIFS share name. You may use the command "smbclient -L x.x.x.x" to query the CIFS share names.

/mnt/temp = local client mount point.

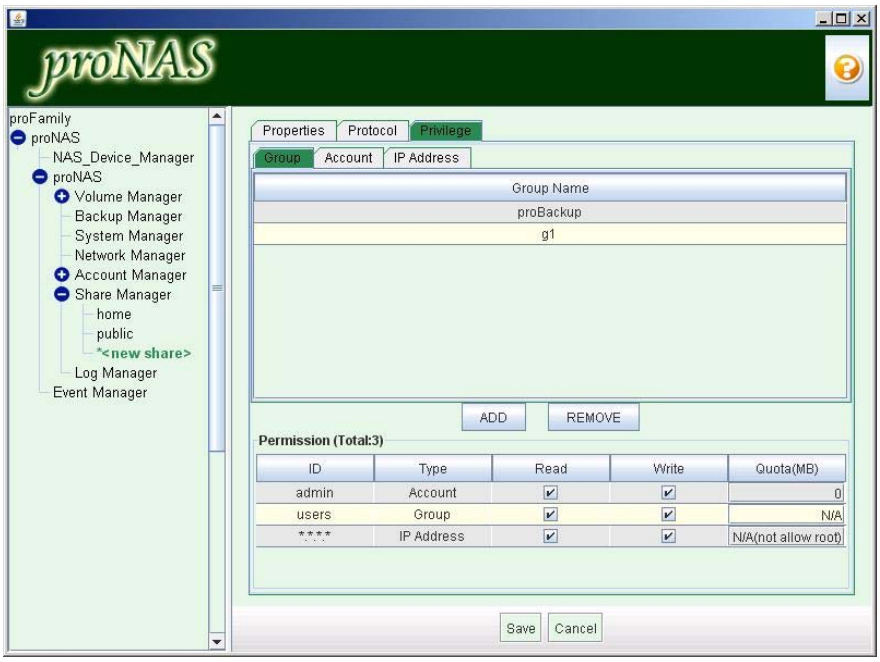
-o username=account,password=secret = the account name and password

5.4.4 Privilege Setting

Using Privilege tab, administrator can set the ACL (Access Control List) for share folder either by Group, Account, or IP Address.

5.4.4.1 Group

You can assign specific group read or read/write permission for certain share folder. Choose the group and press "ADD" button. The group will displayed in the permission list, and check "Read" or "Write" or check both and press "Save". If you would like to remove the group with ACL setting to certain share folder, select the group name and press "REMOVE" button.



Group Name
proBackup
g1

Permission (Total:3)

ID	Type	Read	Write	Quota(MB)
admin	Account	☑	☑	0
users	Group	☑	☑	N/A
..*.*	IP Address	☑	☑	N/A(not allow root)

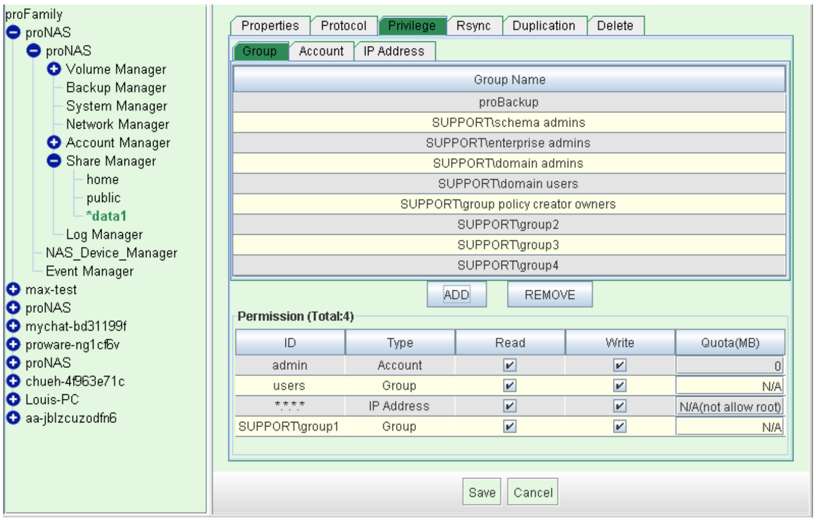
Sample Steps to Assign Group Account Permission to Share:

1. Select Share Manager. Select the share name where account will be given permission, and click Privilege tab.
2. Click “Edit”. Select Group tab.
3. Select the group account that will be given permission and click “ADD”.

NOTE: When group account name is selected, it will be highlighted. If you want to select more than one group account at the same time, press “Shift” key then click the groups you want to add to Permission list.

4. In the Permission list, modify the permission, either Read-Only (no check mark in “Write” box) or Read/Write (both “Read” and “Write” boxes have check marks).

5. Click Save.



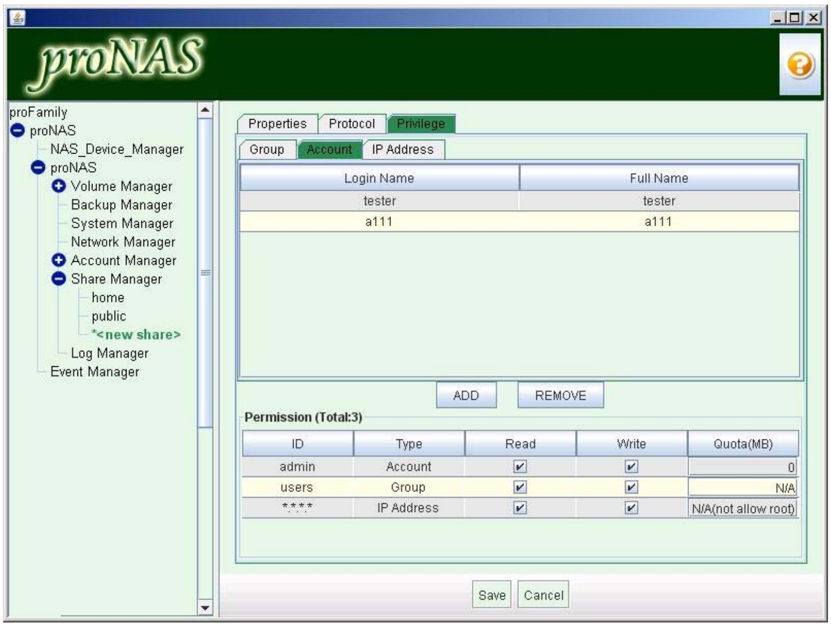
Group Name
proBackup
SUPPORT\schema admins
SUPPORT\enterprise admins
SUPPORT\domain admins
SUPPORT\domain users
SUPPORT\group policy creator owners
SUPPORT\group2
SUPPORT\group3
SUPPORT\group4

Permission (Total:4)

ID	Type	Read	Write	Quota(MB)
admin	Account	☑	☑	0
users	Group	☑	☑	N/A
..*.*	IP Address	☑	☑	N/A(not allow root)
SUPPORT\group1	Group	☑	☑	N/A

5.4.4.2 Account

You can assign specific account user read or read/write permission for certain share folder. When you set the account with ACL, it may be necessary to remove the users group from the permission list in order to prevent access of other members of “users” group to the share. Choose the account and press "ADD" button, and the account will be displayed in the permission list. Check "Read" or "Write" or check both and press "SAVE".



Login Name	Full Name
tester	tester
a111	a111

Permission (Total:3)

ID	Type	Read	Write	Quota(MB)
admin	Account	☑	☑	0
users	Group	☑	☑	N/A
..*.*	IP Address	☑	☑	N/A(not allow root)

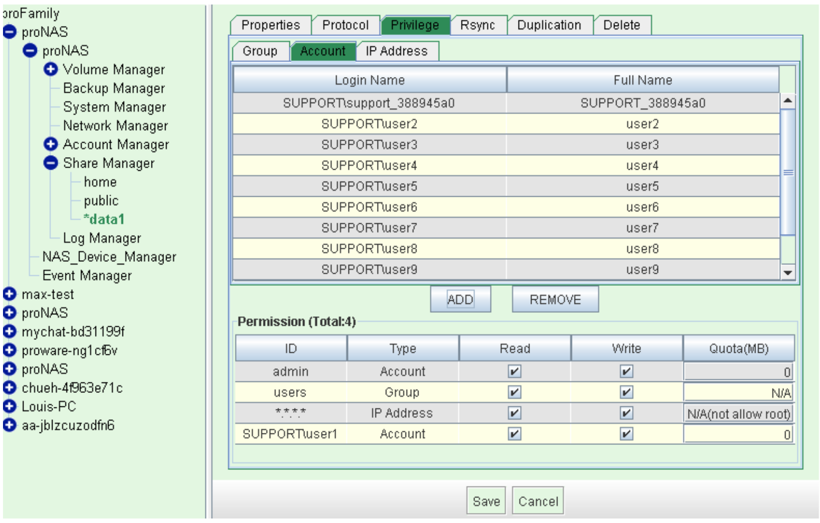
NOTE: Newly added users or groups may have no permissions on the existing files or sub-folders until "Apply ACL" button is executed.

Sample Steps to Assign User Account Permission to Share:

1. Select Share Manager. Select the share name where account will be giver permission, and click Privilege tab.
2. Click “Edit”. Select Account tab.
3. Select the account name that will be given permission and click “ADD”.

NOTE: When account name is selected, it will be highlighted. If you want to select more than one account at the same time, press “Shift” key then click the accounts you want to add to Permission list.

4. In the Permission list, modify the permission, either Read-Only (no check mark in “Write” box) or Read/Write (both “Read” and “Write” boxes have check marks).
5. Click Save.



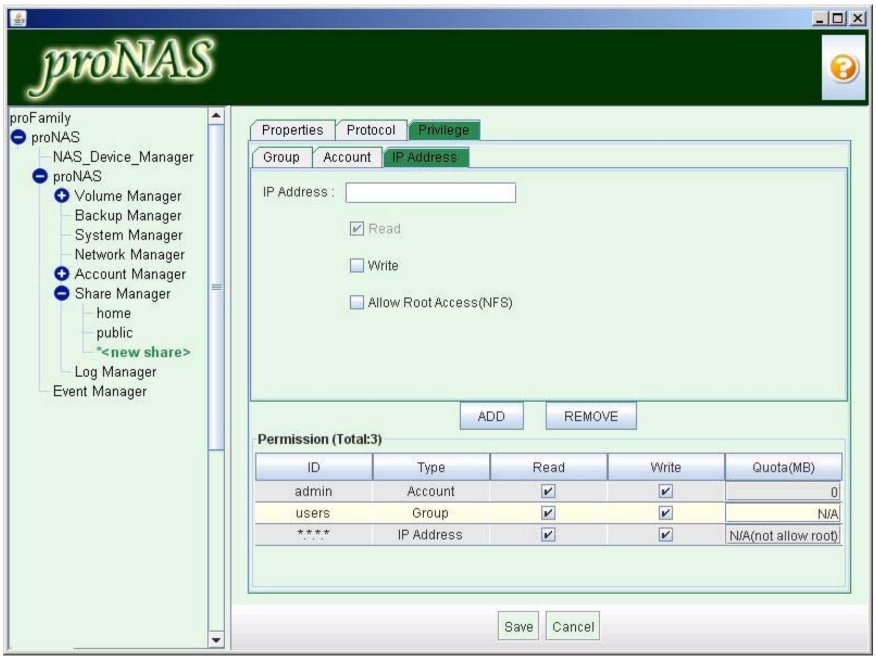
Login Name	Full Name
SUPPORT\support_388945a0	SUPPORT_388945a0
SUPPORT\user2	user2
SUPPORT\user3	user3
SUPPORT\user4	user4
SUPPORT\user5	user5
SUPPORT\user6	user6
SUPPORT\user7	user7
SUPPORT\user8	user8
SUPPORT\user9	user9

Permission (Total:4)

ID	Type	Read	Write	Quota(MB)
admin	Account	☑	☑	0
users	Group	☑	☑	N/A
..*.*	IP Address	☑	☑	N/A(not allow root)
SUPPORT\user1	Account	☑	☑	0

5.4.4.3 IP Address

This option allows you to set a certain range of hosts to have an access into proNAS. By default, the IP address is set to *.*.*.* which means that it will accept connections from any host. If set to 192.168.100.*, this will only allow connections from your private network 192.168.100 and all other connections will be refused.



IP Address :

☑ Read

□ Write

□ Allow Root Access(NFS)

Permission (Total:3)

ID	Type	Read	Write	Quota(MB)
admin	Account	☑	☑	0
users	Group	☑	☑	N/A
..*.*	IP Address	☑	☑	N/A(not allow root)

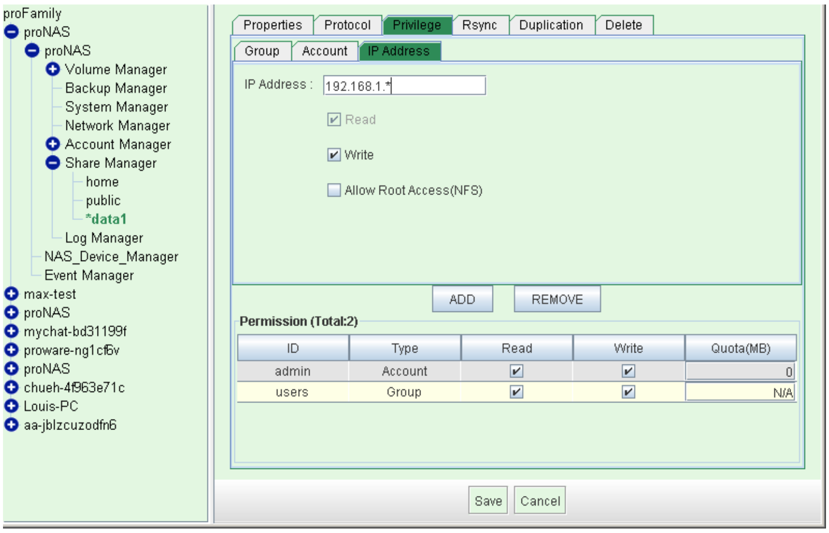
Note: Not all ACL permission settings may be applicable to all share protocols. If you set NFS protocol, it can support all ACL setting mentioned above. If you set CIFS protocol, read only IP address will not be honored. If you set AppleTalk or Netware protocol, you can only set ACL permission by account or group.

Sample Steps to Limit Share Connections to Selected IP Range:

1. Select Share Manager. Select the share name where account will be giver permission, and click Privilege tab.
2. Click "Edit". Select IP Address tab.

   NOTE: BY default, all IP addresses (*.*.*.*) have Read/Write access to the NAS. If you restrict NAS connections from specific IP range, only the selected IP range can access the NAS share. Group Permission or User Account Permission is still needed to be assigned in order for users to gain access to the share folder.
3. To remove *.*.*.*, select "*.*.*.*" from Permission list and click "REMOVE".
4. To add an IP range, enter the IP range (e.g.: 192.168.1.*) in the "IP Address" box, check the "Write" box to assign Read-Write access if necessary, and click "ADD".

5. Click “Save” when done.



IP Address : 192.168.1.*

☑ Read

☑ Write

☐ Allow Root Access(NFS)

Permission (Total:2)

ID	Type	Read	Write	Quota(MB)
admin	Account	☑	☑	0
users	Group	☑	☑	N/A

Permissions:

This section lists the permissions that you can assign for each user, group, or IP address. When you create a share, the default owner which is the "admin" will be granted full control. The same is also true for "users" group and the "*.*.*.*" for IP address.

Listed below are the share permissions defined in proNAS:

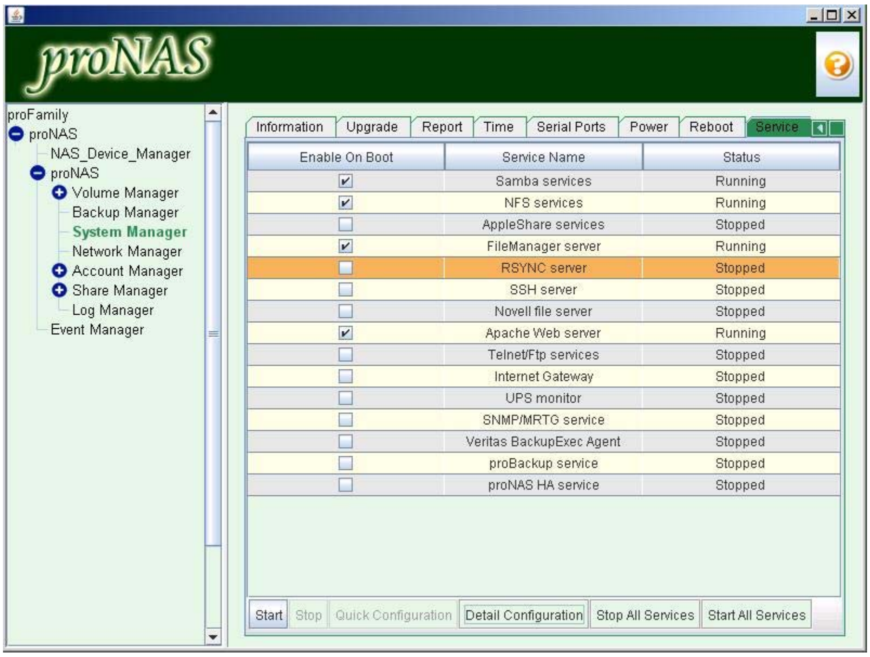
Read Only			**Read+Write**		
	Allow	Deny		Allow	Deny
Access share, sub-folder	☑		Access share, sub-folder	☑	
Read	☑		Read	☑	
Write		☑	Write	☑	
Edit/Modify		☑	Edit/Modify	☑	
Delete		☑	Delete	☑	
Rename		☑	Rename	☑	

Setting the amount of quota to a specific user

In the "Quota(MB)" field, you can input the quota of an account which is granted permission to the share. Press the "Enter" key after you input the amount in Quota(MB) field. To remove the quota limit, set the Quota(MB) to 0 then press "Enter" key.

5.4.5 Rsync

Rsync copies files either to or from a remote host, or locally on the current host. It is also a utility that provides fast incremental file transfer. proNAS Rsync implementation can be set either in server mode or client mode. Server mode means that proNAS can accept incoming Rsync connections, where as in client mode, proNAS is the one who initiates the synchronization. To use as a server mode, you must start the "RSYNC server" first. Go to System Manager -> Service tab, highlight "RSYNC server" then click the "Start" button.



Enable On Boot	Service Name	Status
☑	Samba services	Running
☑	NFS services	Running
□	AppleShare services	Stopped
☑	FileManager server	Running
□	RSYNC server	Stopped
□	SSH server	Stopped
□	Novell file server	Stopped
☑	Apache Web server	Running
□	Telnet/Ftp services	Stopped
□	Internet Gateway	Stopped
□	UPS monitor	Stopped
□	SNMP/MRTG service	Stopped
□	Veritas BackupExec Agent	Stopped
□	proBackup service	Stopped
□	proNAS HA service	Stopped

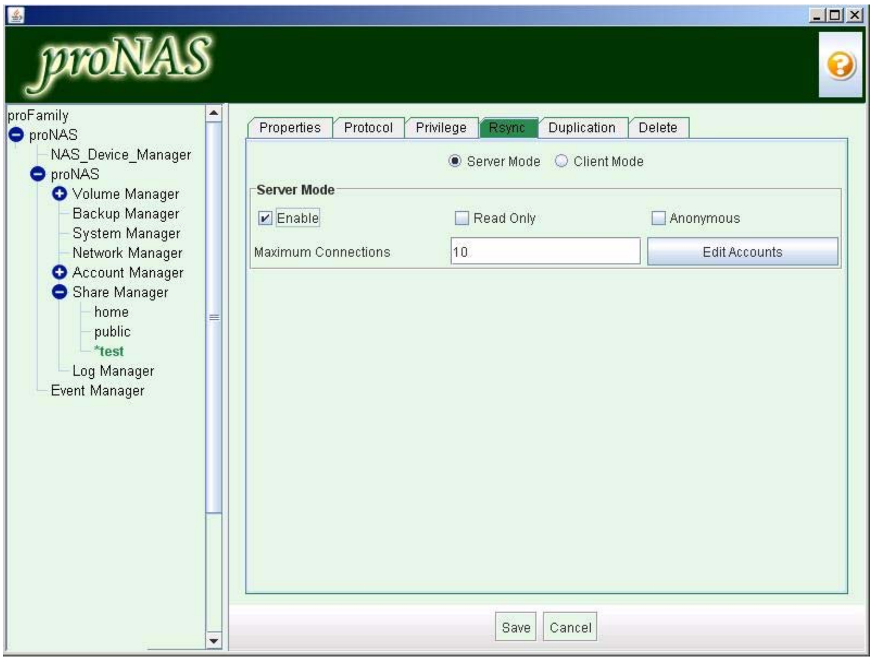
Some of the additional features of Rsync are:

- Support for copying links, devices, owners, groups, and permissions.
- Pipelining of file transfers to minimize latency costs
- Support for anonymous or authenticated Rsync daemons

Server Mode:

When proNAS system is in Server Mode, the Rsync clients can connect either within a local transfer, via a remote shell or via a network socket.

- Enable - When checked, proNAS is set as a Rsync server.
- Read only - When checked, all files within this share will be read only to any Rsync client.
- Anonymous - When checked, anonymous connections will be accepted.
- Maximum Connections - This specifies the maximum number of Rsync client that can connect to this share at a certain time.
- Edit accounts - You may edit and existing account, or add/delete a user. These accounts are the accounts that need to be supplied by the Rsync clients when connecting to this server.



● Server Mode ○ Client Mode

Server Mode

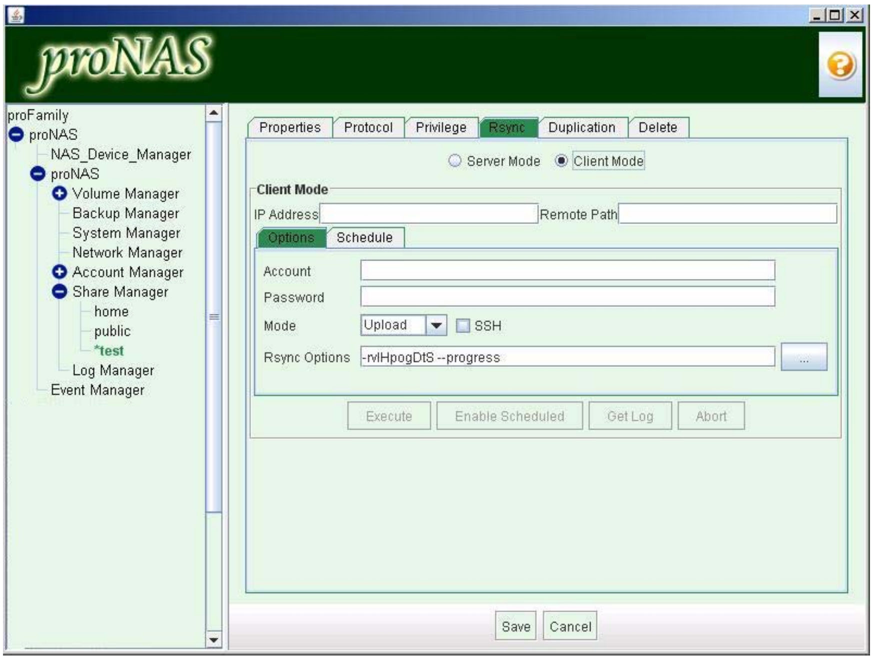
☑ Enable □ Read Only □ Anonymous

Maximum Connections 10

Client Mode:

The proNAS system will initiate the synchronization and contact an Rsync server. There are two different ways for Rsync to contact a remote system: using SSH as a remote-shell program as the transport or contacting an Rsync daemon directly via TCP.

- IP Address - This specifies the IP address of the remote Rsync server.
- Remote Path - This specifies the share on the remote Rsync server.
- Account - The valid account name that will be required by the Rsync server for authentication.
- Password - The account's password.
- Mode - Either to download files from the Rsync server or to upload files into the Rsync server.
- SSH - When checked, SSH service will provide the secure tunnel between an Rsync client and an Rsync server.
- Rsync Options - These are the lists of options used during Rsync file transfer



○ Server Mode ● Client Mode

Client Mode

IP Address:

Remote Path:

Account:

Password:

Mode: Upload □ SSH

Rsync Options: -rvlHpogDtS --progress

Here is a short summary of the available options. Please refer to the detailed description below for a complete description. Some options only have a long variant.

-r, --recursive recurse into directories

-v, --verbose increase verbosity. This option increases the amount of information your are given during the transfer

-l, --links copy symlinks as symlinks

-p, --perms preserve permissions. This option causes the receiving Rsync to set the destination permissions to be the same as the source permissions.

-o, --owner preserve owner (super-user only). This option causes Rsync to set the owner of the destination file to be the same as the source file

-g, --group preserve group. This option causes Rsync to set the group of the destination file to be the same as the source file.

--ignore-existing Ignore files that already exist on the receiver. This tells Rsync to skip updating files that already exist on the destination.

-b, --backup With this option, preexisting destination files are renamed as each file is transferred or deleted. You can control where the backup file goes and what (if any) suffix gets appended using the --backup-dir and --suffix options

--backup-dir=dir In combination with the --backup option, this tells Rsync to store all backups in the specified directory. This is very useful for incremental backups. You can additionally specify a backup suffix using the --suffix option (otherwise the files backed up in the specified directory will keep their original filenames).

--suffix=SUFFIX This option allows you to override the default backup suffix used with the --backup (-b) option. The default suffix is a ~ if no --backup-dir is specified, otherwise it is an empty string.

-D, --devices preserve device files

--specials preserve special files

-t, --times preserve times

-S, --sparse handle sparse files efficiently

-z, --compress Compresses file data during the transfer. This option is useful in slow links.

-a, --archive This is equivalent to -rlptgoD. It is a quick way of saying you want recursion and want to preserve almost everything (with -H being a notable omission).

-E, --executability This option causes Rsync to preserve the executability (or non-executability) of regular files when --perms is not enabled.

-h, --human-readable Output numbers in a human-readable format.

--stats Give some file-transfer stats.

--delete Delete files that don't exist on the sender.

--log-file-format=FORMAT Output filenames using the specified format.

--log-file=FILE Output filenames using the specified file.

--bwlimit=KB/S Limit I/O bandwidth; KBytes per second.

-n, --dry-run This tells Rsync to not do any file transfer; instead it will just report the actions it would have taken.

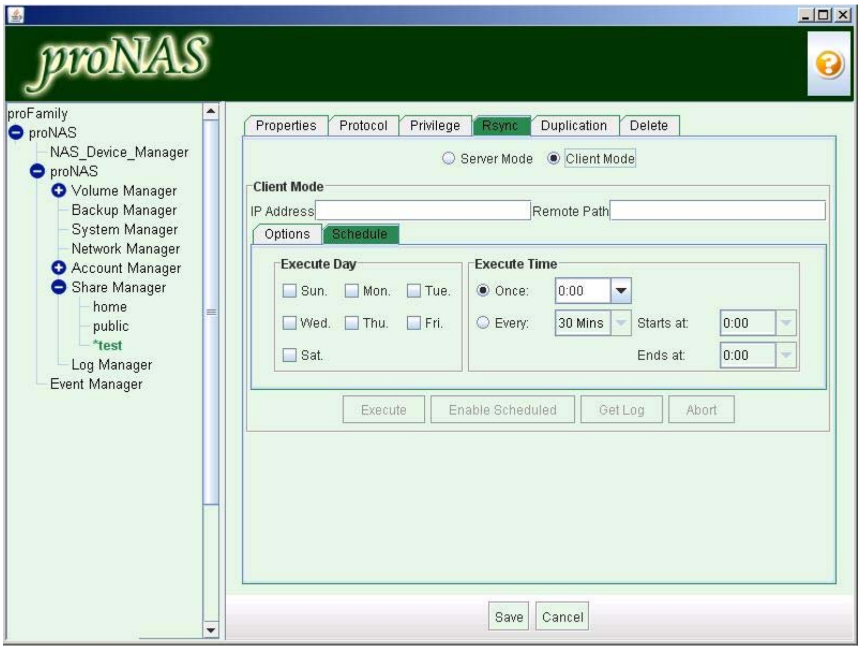
--timeout=SECS Sets the maximum I/O timeout in seconds. If no data is transferred for the specified time then Rsync will exit. The default is 0, which means no timeout.

There are lot more useful options that are not included in this list. It may vary depending on your usage, for more information on Rsync, please visit http://samba.org/rsync/.

After completing the above settings, you can run the Rsync client task immediately by clicking the "Execute" button.

Rsync Schedule

You can automate the Rsync client tasks simply by running it thru schedule. Please select which day(s) to run, the time of the day or if by interval, select a time then set the starting/ending time and then enable the schedule by clicking on the "Enable Scheduled" button.



○ Server Mode ● Client Mode

Client Mode

IP Address Remote Path

Execute Day

□ Sun. □ Mon. □ Tue.

□ Wed. □ Thu. □ Fri.

□ Sat.

Execute Time

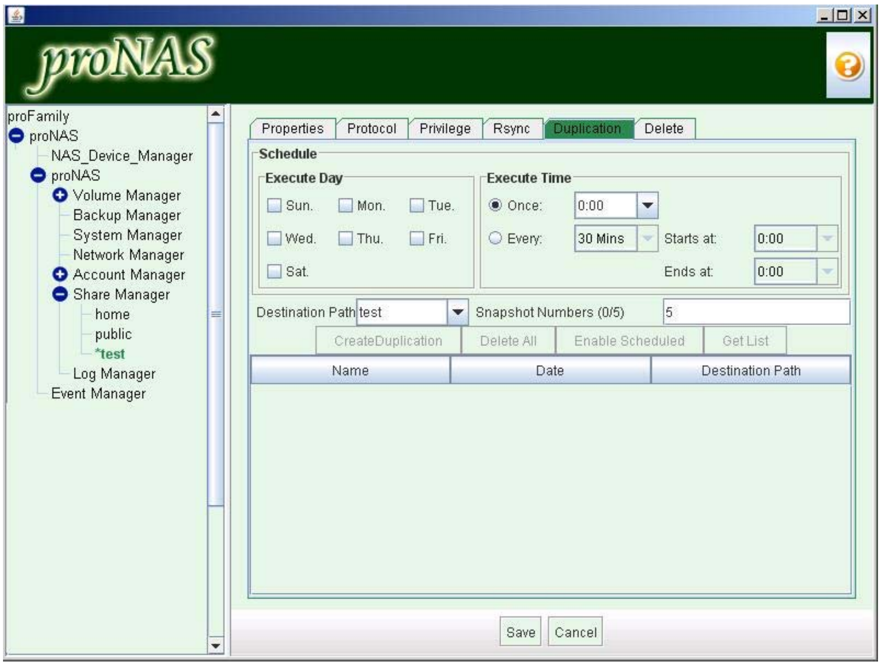
● Once: 0:00

○ Every: 30 Mins Starts at: 0:00

Ends at: 0:00

5.4.6 Duplication

Duplication is a file level snapshot utility for making backups of your local filesystem. Using Duplication, it is possible to take incremental snapshots of your filesystem at different points in time. Duplication creates the illusion of having a multiple full backups by using hard links, while only taking up the space of one full backup plus differences. This saves much more disk space than one might image. The duplication files will be directed to a share which you can access via share protocols or by telnet service. Duplication can be invoked manually or by schedule.
Select the share folder in Share Manager then click “Edit” button.



Schedule

Execute Day

□ Sun. □ Mon. □ Tue.
□ Wed. □ Thu. □ Fri.
□ Sat.

Execute Time

● Once: 0:00
○ Every: 30 Mins Starts at: 0:00
Ends at: 0:00

Destination Path: test Snapshot Numbers (0/5): 5

Creating Duplication by Schedule

To create duplication by schedule, first set the number of total duplication that will be created, specify which day to be run, set the time task whether by interval or once in a specific time of day, set the destination path and then click “Save” button. Enable the schedule by clicking on the "Enable Scheduled" button. To disable the scheduled duplication, just click on the "Disable Scheduled" button.

The Duplication tab information is shown below.

Execute Day: Specifies whether the scheduled task is to run on this day.

Execute Time: **Once** - Specifies the time of the day the scheduled task create the snapshot.
Every - Specifies how often the scheduled task is to be repeated. You can also select the starting time and the ending time.

Destination Path: This will be the location where your duplication files will be saved. The default path will be the path of the share itself. You can change the path to the other shares except home and public. Duplication will follow the ACL settings of the destination share. If you set the destination of your home duplication to a public share then anybody can access that folders, so please be warned!

Snapshot Numbers: Specifies the total number of snapshots that can be created. The maximum total number of duplication a share can have is 256.

Note: The destination space must be larger than the source. proNAS will check only the destination volume size, not the share usage. Be sure that the available space on the destination is reasonably big enough to accommodate any changes in the source. Home duplication is a special case. If the destination path of the home folder is set to the home itself, its duplication files will only be accessible via NFS or telnet service.

Create Duplication: This button allows you to create duplication manually.

Delete All: This button will remove all the duplication files of this share on the current destination path.

Enable / Disable Scheduled: This button allows you to enable or disable a scheduled task.

Get List: This button allows you to get the lists of duplications on the current destination path.

Creating Duplication Manually

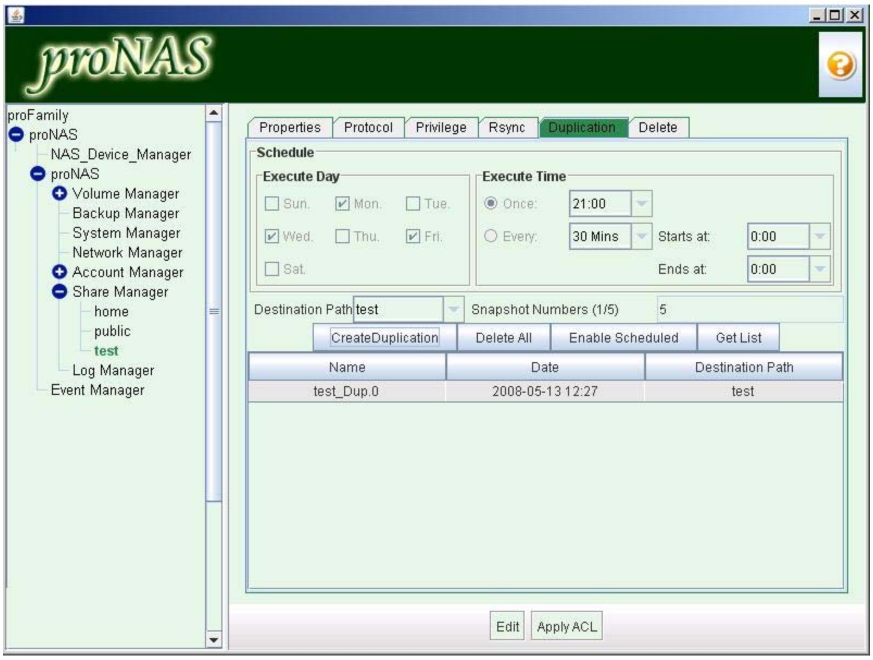
To create duplication manually, first set the number of total duplication that will be created, set the destination path and then click the "CreateDuplication" button. The source share must have at least a single file in order for the duplication to work properly.

Removing or Clearing All Duplication Files

To delete all the duplication files of this share on the current destination path, press the "Delete All" button. Duplication files on the previous destination path will not be removed. Duplication files of other shares on the same destination path will not also be removed.

Getting the Duplication List

To get the lists of all duplication files of this share on the current destination path, please press the "Get List" button. The table will then update the lists of duplication folders. The table includes the date and time it was created and the destination path where it was saved. Duplication files of this share on the previous destination will no longer be included in the list. However proNAS will automatically update the duplication list for you every minute.



Schedule

Execute Day
□ Sun. ☑ Mon. □ Tue.
☑ Wed. □ Thu. ☑ Fri.
□ Sat.

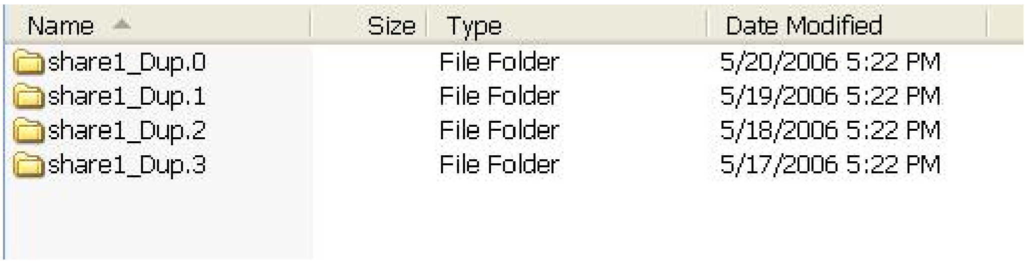
Execute Time
● Once: 21:00
○ Every: 30 Mins Starts at: 0:00
Ends at: 0:00

Destination Path test
Snapshot Numbers (1/5) 5

Name	Date	Destination Path
test_Dup.0	2008-05-13 12:27	test

How Duplication Works

After you have created Duplication, your destination path will contain a folder "._Duplication". (It is hidden by default, to unhide it, uncheck the "hide duplication" option in the Properties tab of the destination folder). Inside the "._Duplication" folder are the directories that are created for the various intervals that you have defined. It will look something like in the figure below.



Name	Size	Type	Date Modified
share1_Dup.0		File Folder	5/20/2006 5:22 PM
share1_Dup.1		File Folder	5/19/2006 5:22 PM
share1_Dup.2		File Folder	5/18/2006 5:22 PM
share1_Dup.3		File Folder	5/17/2006 5:22 PM

Inside each of these folders is the full backup of that point in time of the source share. The format of the duplication folder name will be the share name of the source share appended by an underscore then the character "Dup" followed by the number of the interval. "ShareName_Dup.0" will always contain the most recent snapshot and the duplication with the highest interval number will contain the oldest snapshot. When a new duplication is run, it will rotate all the duplication directories. The files on oldest duplication will not be saved and will be replaced with the content of its succeeding duplication, so please take note of this. The number of duplication will depend on the number of snapshots that you have defined. You need to increase the total number of snapshots if you want to save the backups for a longer time. For example, if you set the snapshot numbers to 60 and you set a schedule to take duplication every day, the very last backup would be around two months old before it will be discharged if a new duplication is made.

NOTE: To view the date modified of duplication folders that corresponds to the date the duplication is taken, use File Manager and view in detailed mode.

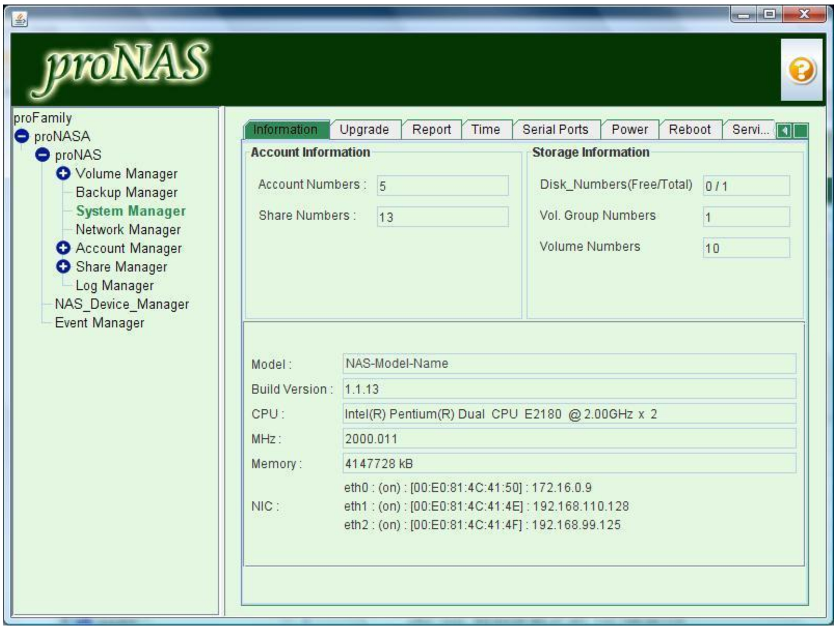
5.4.7 Default Share

Basically, there are there are only two default shares when proNASVG is initially created. If the proBackup Service is started, two other default shares are created. The default shares in proNAS are:

- home - holds the individual shares of all users. It cannot be deleted.
- public - a share intended for all users. Any type of user (including guests or anonymous) can logon to this share and is given read-write permissions.
- proBackupDevice - holds the major backup device for proBackup application. It becomes visible after proBackup service is enabled.
- proBackupExtendedDevice - holds the extended device for other proBackup servers to utilize. It becomes visible after proBackup service is enabled.

5.5 System Manager

System Manager is composed of different tabs which is responsible for the configuration of proNAS system settings and services, such as: Firmware Upgrade, Account and Share reports, Date and Time Zone, Serial Ports and UPS settings, Reboot functions, and Services configurations.



Account Information

Account Numbers : 5

Share Numbers : 13

Storage Information

Disk_Numbers(Free/Total) 0 / 1

Vol. Group Numbers 1

Volume Numbers 10

Model : NAS-Model-Name

Build Version : 1.1.13

CPU : Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz x 2

MHz : 2000.011

Memory : 4147728 kB

NIC :
eth0 : (on) : [00:E0:81:4C:41:50] : 172.16.0.9
eth1 : (on) : [00:E0:81:4C:41:4E] : 192.168.110.128
eth2 : (on) : [00:E0:81:4C:41:4F] : 192.168.99.125

5.5.1 Information tab

The Information tab shows the account, storage and system information.

Account Information

- **Account Numbers** - Indicates the total numbers of all local and external accounts.
- **Share Numbers** - Indicates the total number of all shares.

Storage Information

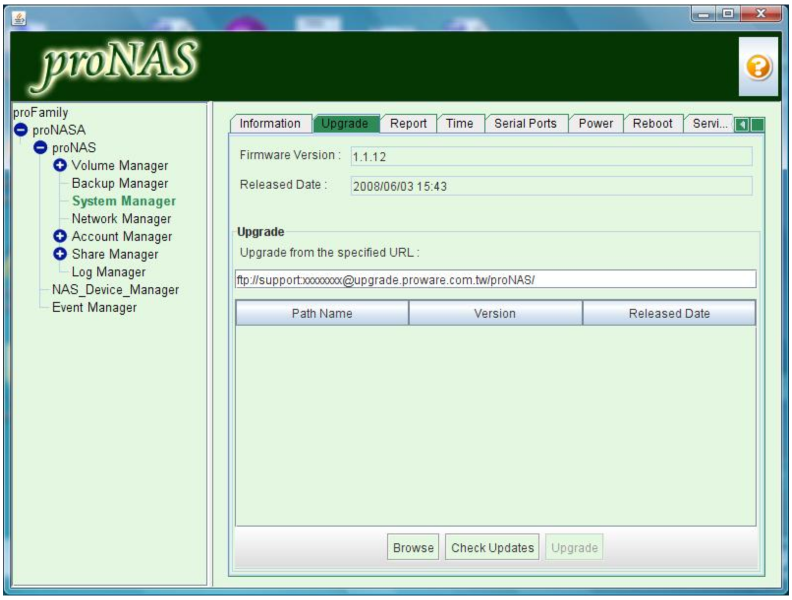
- **Disk Numbers (Free/Total)** - The number of disks in the subsystem, "Free" means the disks those are not joined in volume group.
- **Vol Group Numbers** - The total number of volume groups.
- **Volume Numbers** - The total number of logical volumes. Snapshots will also be counted as volumes.

System Information

- **Model -** Specifies the proNAS system model type.
- **CPU** - Specifies the CPU Type and the number of CPUs.
- **MHz** - Specifies the CPU speed.
- **Memory** - Memory size.
- **NIC** - NIC status, MAC address and IP address.
- **Build Version** - proNAS current firmware version.

5.5.2 Upgrade tab

The Upgrade tab is used to upgrade the proNAS system firmware version.



Firmware Version : 1.1.12

Released Date : 2008/06/03 15:43

Upgrade

Upgrade from the specified URL :

ftp://support:xxxxxxxx@upgrade.proware.com.tw/proNAS/

Path Name	Version	Released Date

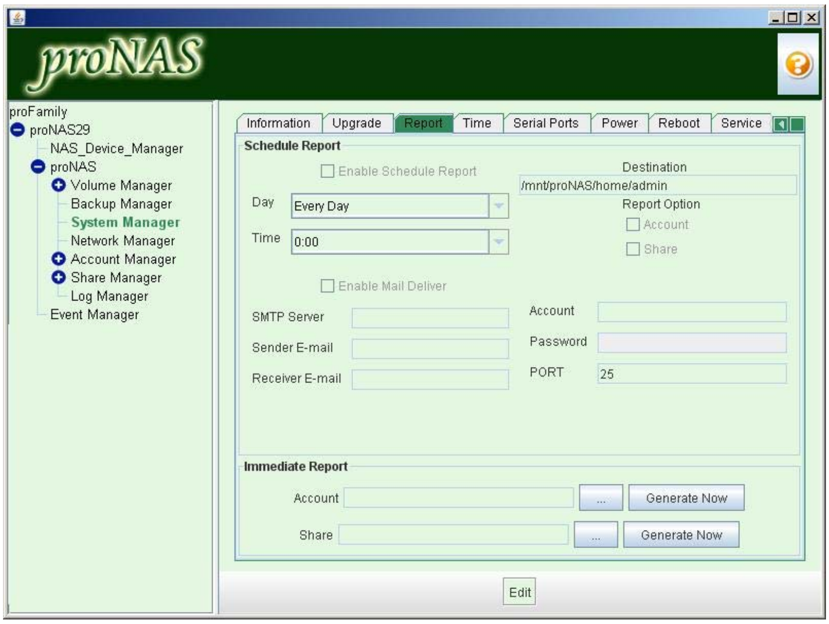
- **Firmware Version** - Displays the current firmware version.
- **Release Date** - The Release Date of this version.
- **Upgrade from the specified URL** - You can download the latest version from URL: ftp://support:xxxxxxxx@upgrade.proware.com.tw/proNAS/

If you would like to see if there is latest version, please press "Check Updates" button. The system will search if there is any latest firmware to update.

Besides firmware update from web-site, you can also do a firmware update from local file system, but you need to download first the firmware Patch and save to the local file system. Press "Browse" button and locate the firmware patch.

5.5.3 Report tab

proNAS provides report function which enables you to collect the usage information of all accounts and shares. The output file will be saved in a ".csv" file. Report function can generate report either by schedule or immediately.



Schedule Report

□ Enable Schedule Report

Day: Every Day

Time: 0:00

Destination: /mnt/proNAS/home/admin

Report Option: □ Account □ Share

□ Enable Mail Deliver

SMTP Server:

Sender E-mail:

Receiver E-mail:

Account:

Password:

PORT: 25

Immediate Report

Account: ...

Share: ...

Schedule Report

If you would like to enable schedule report, press the "Edit" button, check "Enable Schedule Report", check the report option for "Account" or "Share" or both, and set the Day and Time when to generate the report. The system will generate the report and save in the path /mnt/proNAS/home/admin (The path can be modified).

If you would like to receive the report by e-mail, please check "Enable Mail Deliver" and input the information for SMTP server, sender e-mail and receiver e-mail address. If you prefer to enable email authentication, enter the account and password. You can also change the default port if needed.

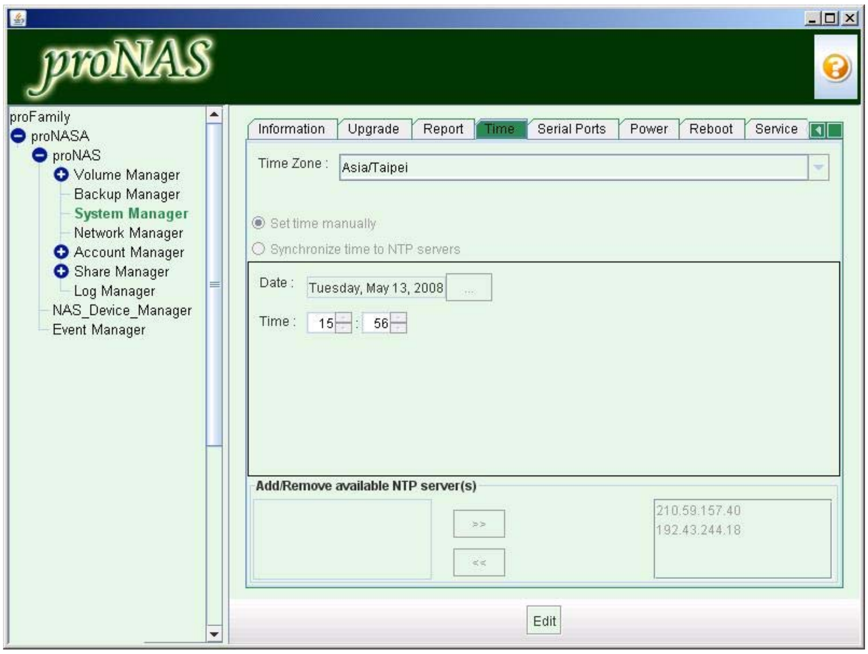
Immediate Report

If you would like to collect the report immediately, press "..." and choose the path for the output file and press "Generate Now" button.

5.5.4 Time tab

You can configure the system time, date and time zone in this tab. Click the "Edit" button and choose the appropriate time zone. After setting the time zone, select "Set time manually", if not selected, then set the Date and Time. To set the date, press "...", then the system will display a calendar to choose the date.

If you would like to synchronize time with NTP server, select "Synchronize time to NTP server". The system will display two NTP servers by default. If you would like to add NTP server, press ">>", or press "<<" to remove the NTP server". When the settings are completed, press "Save" button.



Time Zone : Asia/Taipei

● Set time manually

○ Synchronize time to NTP servers

Date : Tuesday, May 13, 2008 ...

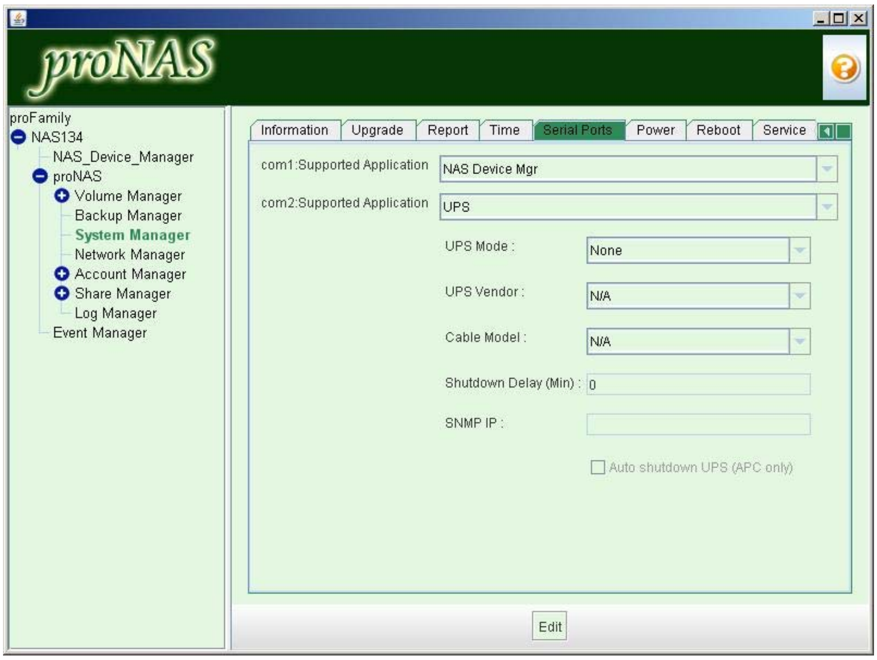
Time : 15 : 56

Add/Remove available NTP server(s)

210.59.157.40
192.43.244.18

5.5.5 Serial Ports tab

Com1 and Com2 Serial ports can be configured in this tab for specific application. Press "Edit".



com1:Supported Application: NAS Device Mgr

com2:Supported Application: UPS

UPS Mode : None

UPS Vendor : N/A

Cable Model : N/A

Shutdown Delay (Min) : 0

SNMP IP :

□ Auto shutdown UPS (APC only)

Com1

Supported Applications are: NAS Device Mgr or proNAS HA

Com2

Supported Applications are: UPS or proNAS HA

If you set Com2 to UPS, you can select between two supported **UPS Modes:** dumb mode or smart mode.

If you choose dumb mode, you don't have to configure the detail setting about vendor and cable. If you choose smart mode, proNAS supports three **UPS Vendor:** (a) APC, (b) BeamTech, and (c) HyperPro. Select the UPS vendor then set the **UPS Model** and **Cable Model**. The only Beamtech UPS model supported is SSpro 650. The only HyperPro UPS model supported is 1410HP. APC has many models supported. APC cable models are: simple, smart, ether, usb, and snmp

Shut Down delay (Min): the time to shutdown system after power fail

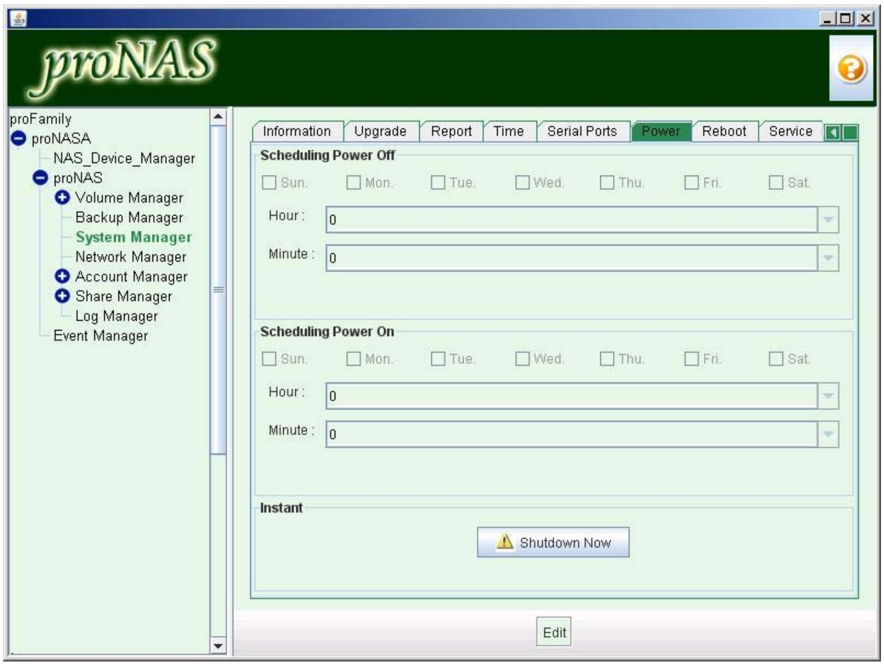
SNMP IP: the IP address of APC UPS. This is enabled when cable model is set to snmp.

Auto Shutdown UPS (APC only): automatically shutdown system after power fail; APC UPS only

After completing the settings, press "Save" button.

5.5.6 Power tab

The Power tab is used to configure schedule system power off and power on. You can also shutdown the system immediately using “Shutdown Now” button.



Scheduling Power Off

□ Sun. □ Mon. □ Tue. □ Wed. □ Thu. □ Fri. □ Sat.

Hour : 0

Minute : 0

Scheduling Power On

□ Sun. □ Mon. □ Tue. □ Wed. □ Thu. □ Fri. □ Sat.

Hour : 0

Minute : 0

Instant

Scheduling Power Off

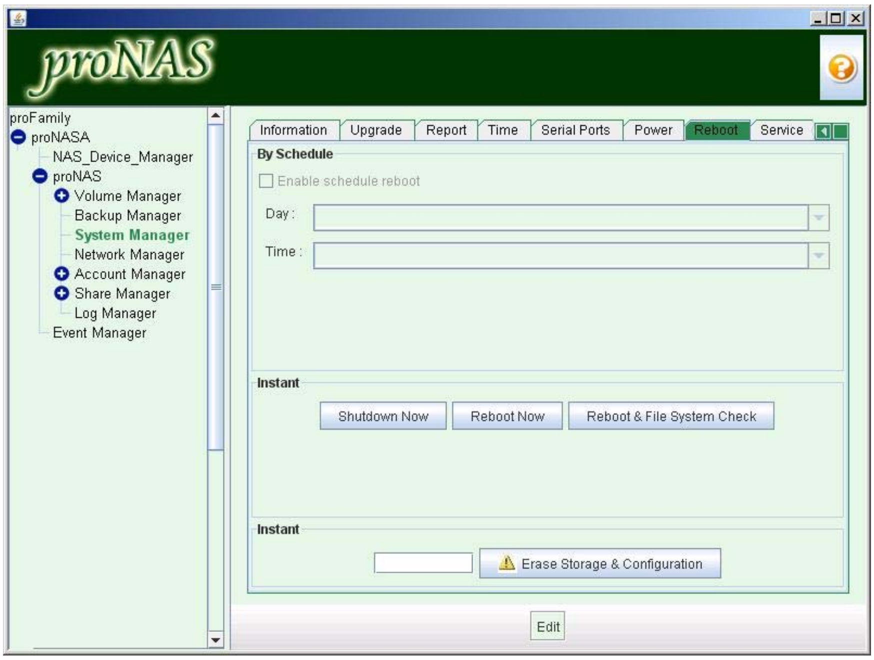
Select the day or days, and set the Hour and Minute when the system will shutdown.

Scheduling Power On

Select the day or days, and set the Hour and Minute when the system will power on.

5.5.7 Reboot tab

The administrator can reboot proNAS by schedule or immediately.



□ Enable schedule reboot

Day :

Time :

If you would like to reboot by schedule, press "**Edit**" button, and check "**Enable schedule reboot**". Choose the date and time when to reboot. This function can help to clean the unnecessary system process or connection periodically.

If you would like to shut down or reboot immediately, press "**Shutdown Now**" or "**Reboot Now**":

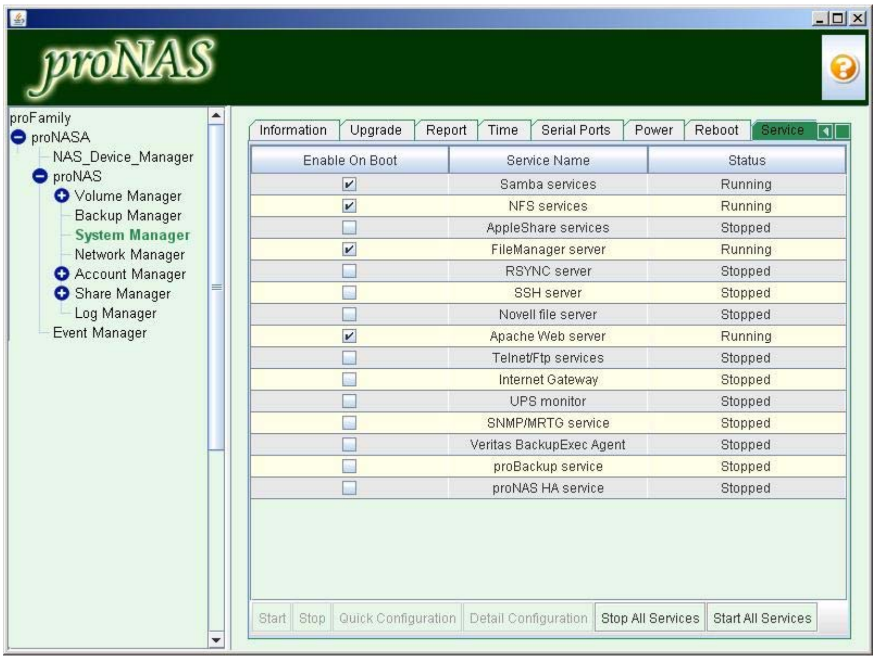
If you check there is file error or I/O error from system log, or VG cannot mount, or system shutdown abnormally, it is recommended to use the function “**Reboot & File System Check**”.

If you would like to erase existing storage and proNAS configuration and reset to factory default, you can use the “**Erase Storage & Configuration**” button.

⚠ **WARNING! All data and configuration will be deleted if you use this function. Please make sure you already have a backup of your data and configuration, or that you do not need the current data and configuration.**

5.5.8 Service tab

The various proNAS services can be set in this tab.



Enable On Boot	Service Name	Status
☑	Samba services	Running
☑	NFS services	Running
□	AppleShare services	Stopped
☑	FileManager server	Running
□	RSYNC server	Stopped
□	SSH server	Stopped
□	Novell file server	Stopped
☑	Apache Web server	Running
□	Telnet/Ftp services	Stopped
□	Internet Gateway	Stopped
□	UPS monitor	Stopped
□	SNMP/MRTG service	Stopped
□	Veritas BackupExec Agent	Stopped
□	proBackup service	Stopped
□	proNAS HA service	Stopped

If you would like to enable service while booting, please check "Enable on Boot" option. You can also press "Start All Services" button to run all services, or press "Stop All Services" button to stop all services. If you would like to enable or disable certain service, please select the service item and press "Start" button or "Stop" button.

The proNAS System services are as follows:

Samba services:	Provides CIFS file sharing, MS Windows users need the this to access proNAS.
NFS service:	Provides NFS file sharing, UNIX users need this to access proNAS.
AppleShare service:	Provides AppleTalk sharing, Mac OS users need this to access proNAS.
FileManager server:	Enables to stop and start the File Manager web page service.
RSYNC server:	Provides Rsync process or system to which the Rsync client connects.
Novell file server:	Provides Netware file sharing, Novell users need this to access proNAS.
SSH server:	Provides remote management with more secure level.
Apache Web server:	Provides web service, you have to enable this service, port number default is 80.

<table>
<tr><td><b>Telnet/Ftp service:</b></td><td>Provides users access proNAS with telnet or ftp</td></tr>
<tr><td><b>Internet Gateway:</b></td><td>Provides Internet access.</td></tr>
<tr><td><b>UPS monitor:</b></td><td>If you would like to connect UPS, you have to enable this service.</td></tr>
<tr><td><b>SNMP/MRTG service:</b></td><td>Provides SNMP/MRTG service to view system information. proNAS can send SNMP traps for the following events:
<table>
<tr><th>Event</th><th>Purpose</th></tr>
<tr><td>Web service stopped (ID 256)</td><td>Notify if Apache web service is stopped.</td></tr>
<tr><td>Logical Volume is Over Quota (ID 128)</td><td>Notify if a logical volumes exceeds the given quota.</td></tr>
<tr><td>Invalid Snapshot (ID 129</td><td>Notify if a snapshot volume is almost full, and it will become invalid.</td></tr>
<tr><td>Replication is Disconnected (ID 130)</td><td>Notify if replication was disconnected.</td></tr>
<tr><td>RAID Fail</td><td>Notify is a RAID Set or Volume Set fails.</td></tr>
<tr><td>Fan Fail</td><td>Notify if a fan fails.</td></tr>
<tr><td>Power Fail</td><td>Notify if a power supply fails.</td></tr>
<tr><td>Disk Fail</td><td>Notify if a disk drive fails.</td></tr>
</table>
</td></tr>
<tr><td><b>Veritas BackupExec eng:</b></td><td>Provides service for Veritas console to make proNAS a Veritas Backup media node.</td></tr>
<tr><td><b>proBackup service:</b></td><td>Provides service for NAS users to backup their files to NAS.</td></tr>
<tr><td><b>proNAS HA service:</b></td><td>Provides NAS HA solution.</td></tr>
</table>

proNAS provides "Quick Configuration" for administrator to configure service parameters. Experienced administrator can also configure the advance settings in "Detail Configuration".

proNAS Quick Configuration options are as follows:

Samba Service

- Strict allocate setting – This option controls the handling of disk space allocation in the proNAS server. When strict allocate is set to “no” (default setting) the server does sparse disk block allocation when a file is extended.

AppleShare Service

- Languages – set the language used for Apple Share service

proBackup Service

- IP of Rx/Tx backup streams: Enter the proNAS network interface IP address for proBackup service stream
- Port of Rx/Tx backup streams: Enter the Port number for proBackup stream , default is 1089.

SSH Service

- Allows root login via SSH service
- Enable SFTP

Apache Web Service

- Default port number is 80

Telnet/FTP services

- Allows root login via FTP
- Allows root login via Telnet

Veritas BackupExec eng service

- Advertised Host: Name of media node
- Workstation password: Administrator password

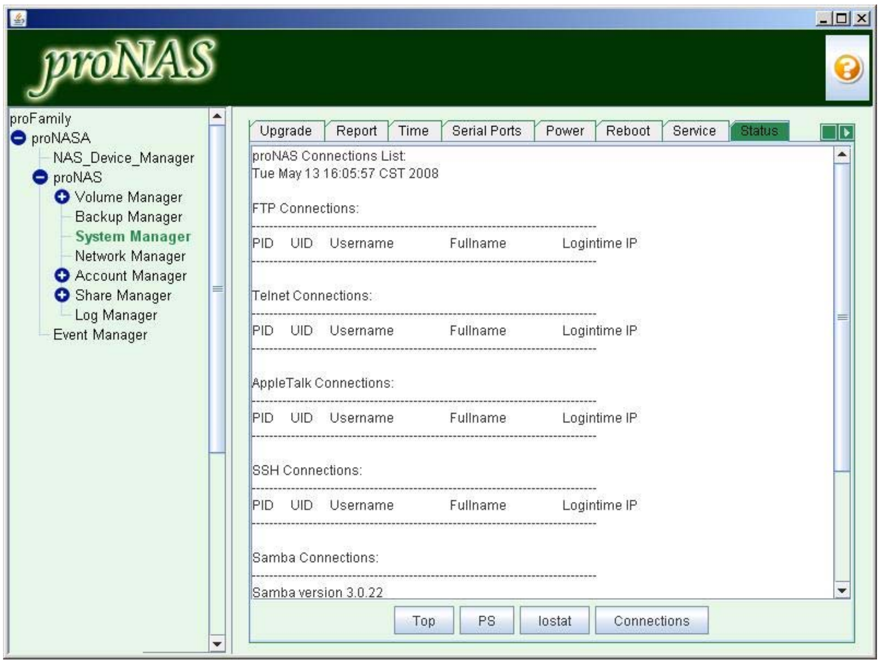
SNMP/MRTG Service

- Trap Receiver IP: Enter the IP address of the SNMP trap receiver.

5.5.9 Status tab

You can use this tab to view system status, such as various Service Connections, Top, PS, and Iostat.

By default, a summary of connections and resources used for local and remote computers is listed. The information includes the PID, User, User full name or comment, login time, and the IP address of the connected computer. You can click the “Connections” button to display current connection list.



```
proNAS Connections List:
Tue May 13 16:05:57 CST 2008

FTP Connections:
------------------------------------------------------------------------------------
PID   UID   Username          Fullname          Logintime IP
------------------------------------------------------------------------------------

Telnet Connections:
------------------------------------------------------------------------------------
PID   UID   Username          Fullname          Logintime IP
------------------------------------------------------------------------------------

AppleTalk Connections:
------------------------------------------------------------------------------------
PID   UID   Username          Fullname          Logintime IP
------------------------------------------------------------------------------------

SSH Connections:
------------------------------------------------------------------------------------
PID   UID   Username          Fullname          Logintime IP
------------------------------------------------------------------------------------

Samba Connections:
------------------------------------------------------------------------------------
Samba version 3.0.22
```

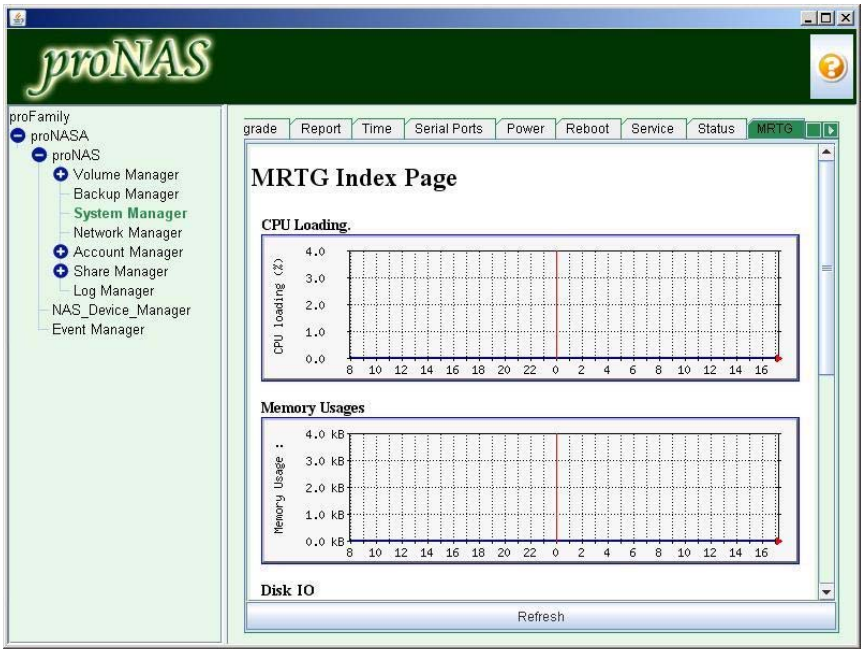
Click the “Top” button to display system summary information and tasks list.

Click the “PS” button to display information about active processes.

Click the “Iostat” button to display system input/output device loading, specifically storage and disk device statistics.

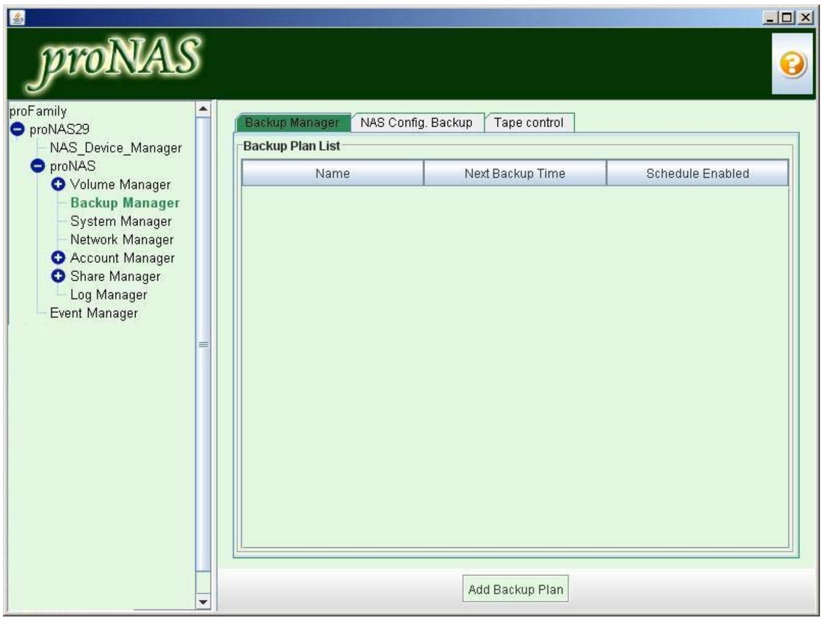
5.5.10 MRTG tab

This tab shows information about MRTG graphs and includes CPU Loading, Memory Usage, Disk IO, and Network Traffic.



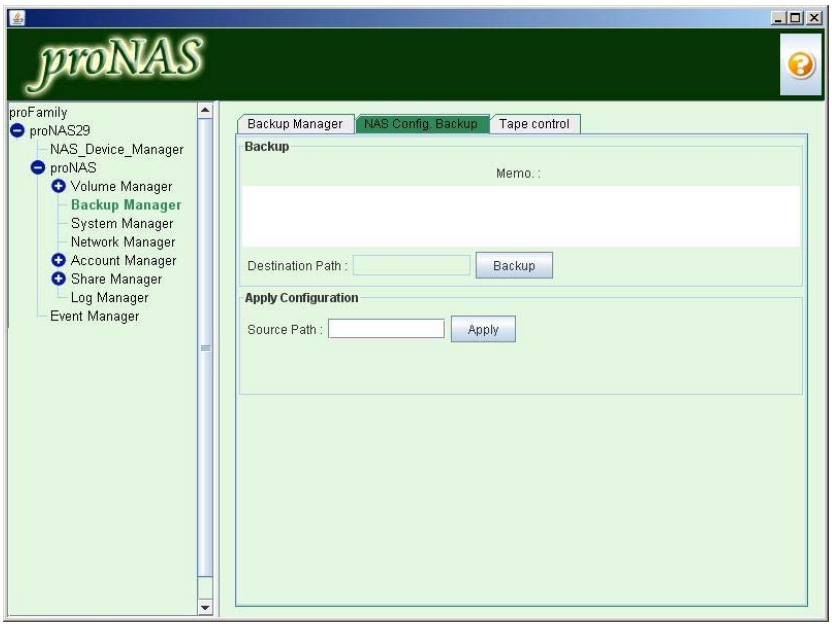
5.6 Backup Manager

You can backup proNAS data and system configuration via Backup Manager.
In "Backup Manager" tab, you can check the existing backup plans in the "Backup Plan List" which includes backup plan name, next backup time and if the backup plan schedule is enabled. If you would like to create new backup plan, please press "Add Backup Plan" button.



5.6.1 proNAS Configuration Backup

proNAS provides System Configuration Backup which means administrator can backup system configuration information. Select "NAS Config Backup" tab.



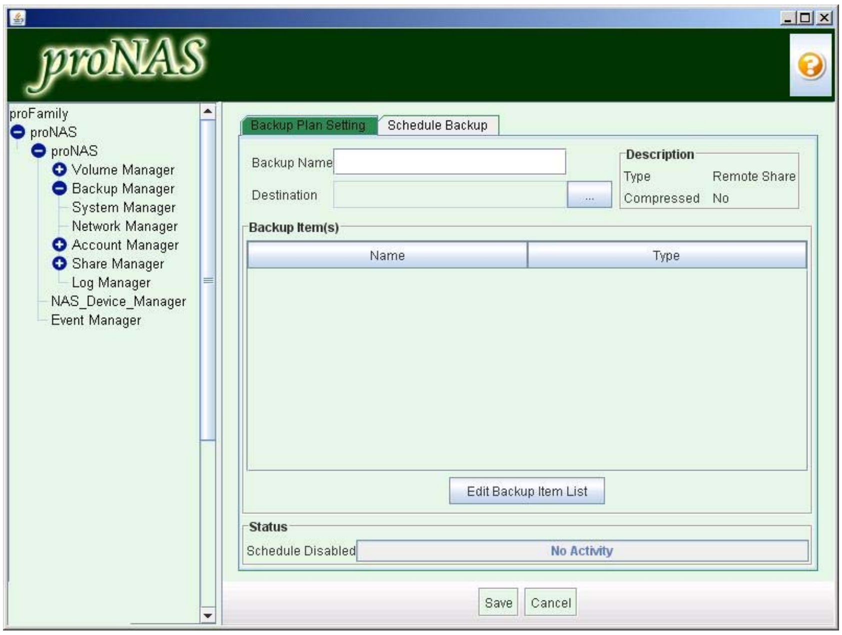
Press "Backup" button. Choose the path you would like to save the file and enter the file name. System will backup the configuration information as an .xml file. If you would like to restore the configuration later, press "Apply" button.

NOTE: Not all proNAS configuration will be included in NAS Config backup. These includes replication, snapshot, Event Manager setting and HA configurations.

NOTE: In order to restore a NAS backup configuration, you need to reset the NAS to factory default settings.

5.6.2 Configure Backup Plan

Backup Plan Setting



Backup Name

Destination ...

Description

Type	Remote Share
Compressed	No

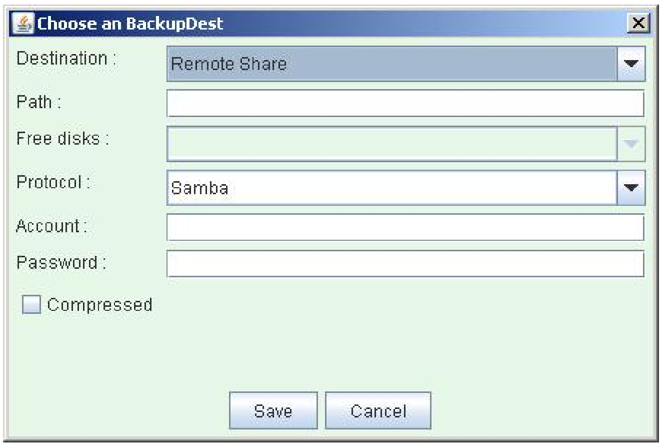
Backup Item(s)

Name	Type

Status

Schedule Disabled No Activity

In the "Backup Plan Setting" tab, you can create new a backup plan. Enter the "Backup Plan Name", and then press "..." to choose the backup destination, your destination could be remote share, tape or local device.



Choose an BackupDest

Destination : Remote Share

Path :

Free disks :

Protocol : Samba

Account :

Password :

□ Compressed

Use the following guidelines to ensure that you are using a valid backup plan name:

- Names cannot be longer than 256 characters.
- Names should be unique. It cannot be a duplicate with other Backup plan names.
- Names cannot contain blank spaces.
- Names cannot begin with a dash (-) and cannot consist of only a single dash.
- Names cannot contain the following characters: /\[]";:|<>+=,?*

If you choose remote share, please input the IP address in the "path" field. Choose Samba or NFS of the protocol and enter account and password.
Example:

For Samba:

Path = //192.168.100.164/Share

You cannot use the directory under the share.
Example:
//192.168.100.164/Share/dir1 <==Incorrect
//192.168.100.164/Share <==Correct
If you are not sure of the share name on the remote machine, you may query it by using the command "smbclient".

```
-bash-3.00# smbclient -L 192.168.100.164
```

Login = account

Account that has full access permission on the remote share.

For NFS:

Path = 192.168.100.164:/PathToShareName

Example:
192.168.100.164:/mnt/proNAS/vol1/share1
If you are not sure of the correct path of the remote NFS server, you may use the command "showmount".

```
-bash-3.00# showmount -e 192.168.100.164
```

Login

For NFS, it will assume the root account to be used. Please verify that root account can access the remote NFS share.

If Backup Manager fails to mount the remote share, you may need to verify it manually via console. That is to connect to the remote machine and mount the remote share. First we need to create a directory as our mount point.

```
-bash-3.00# mkdir /mnt/temp/
```

For Samba:

```
-bash-3.00# mount //ServerIP/ShareName /mnt/temp -o lfs,
                                             username=account,password=password
```

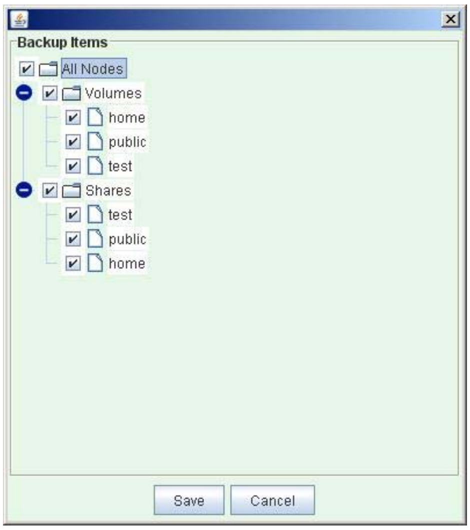
For NFS:

```
-bash-3.00# mount ServerIP:/PathToShareName /mnt/temp
```

If you choose tape, you don't need additional setting.
If you choose local device, the system will display the available disks in the "Free Disk" field.
If you choose the option "compressed", the data will be compressed to * .gz file.

Press "Save" button complete the setting and go back to "Backup Plan Setting" tab. In the field of "Description", system will display you backup destination (remote share / tape / local disk) in Type area.

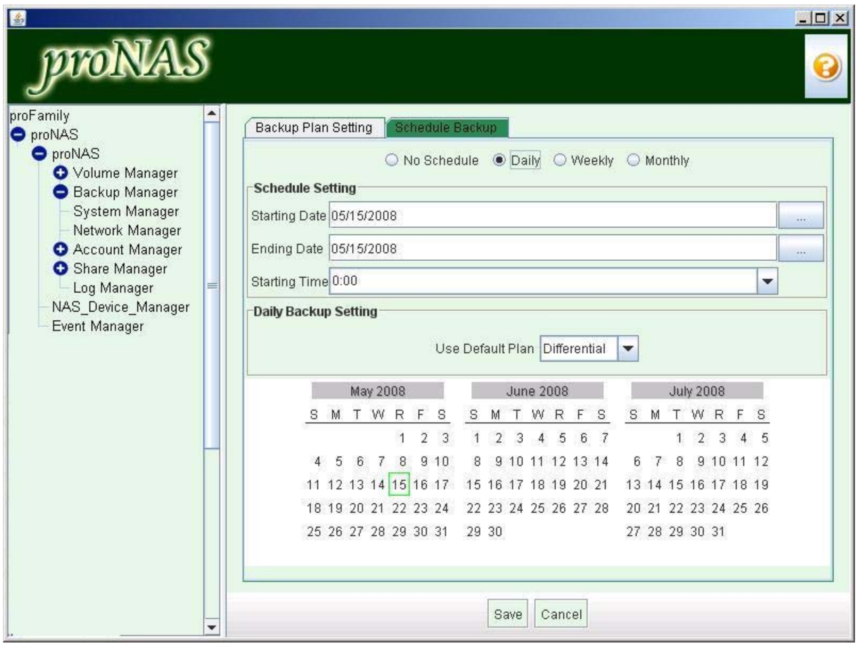
Please press "Edit Backup Item List" button. System will display the window for you to choose the backup items ("Volumes" or "Share"). Choose your backup items and press "Save" button to go back to "Backup Plan Seting" tab. You can check the backup items in the "Backup Item(s)" list, if you would like to remove some items. Please check in the "Remove" filed and press "Remove Backup Item(s)".



Schedule Backup tab

After you complete the above setting, you can setup the schedule in the "Schedule Backup" tab, if the tab, you will see the option of "No Schedule", "Daily", "Weekly", and "Monthly".

- **Daily**: If you would like to do the backup every day, please check "Daily". Please press"...", system will display the calendar. You can choose "Start Date" and "Ending Date" and the "Starting time".



○ No Schedule ● Daily ○ Weekly ○ Monthly

Schedule Setting

Starting Date 05/15/2008

Ending Date 05/15/2008

Starting Time 0:00

Daily Backup Setting

Use Default Plan Differential

May 2008

S	M	T	W	R	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

June 2008

S	M	T	W	R	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

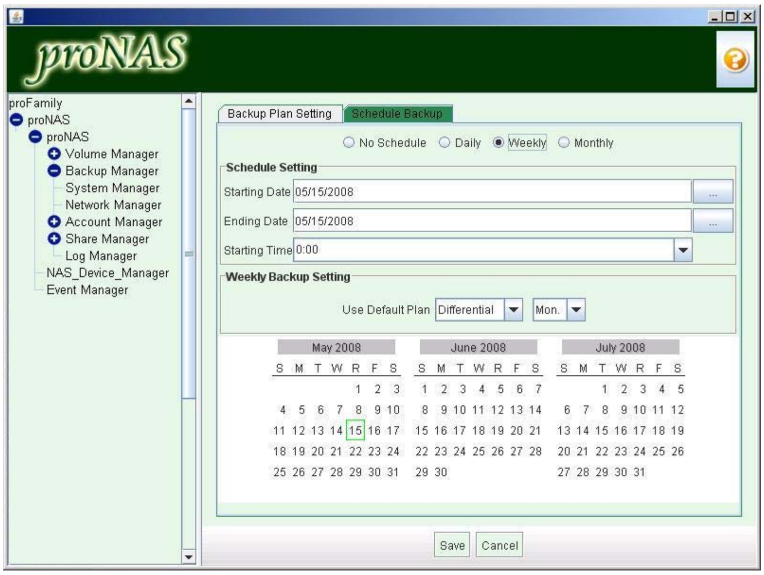
July 2008

S	M	T	W	R	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

proNAS provides 3 kinds of backup methods:

- Incremental: An incremental backup stores all files that have changed since the last backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup is processed, which could result in a lengthy restore job.
- Differential: A differential backup contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if you perform the differential backup too many times, the size of the differential backup might grow to be larger than the baseline full backup.
- Full: Full backup

- **Weekly**: If you would like to backup weekly, please check this option. Please press "...", system will displays the calendar. You can choose "Start Date" and "Ending Date" and the "Starting time".



○ No Schedule ○ Daily ● Weekly ○ Monthly

Schedule Setting

Starting Date 05/15/2008

Ending Date 05/15/2008

Starting Time 0:00

Weekly Backup Setting

Use Default Plan Differential Mon.

May 2008

S	M	T	W	R	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

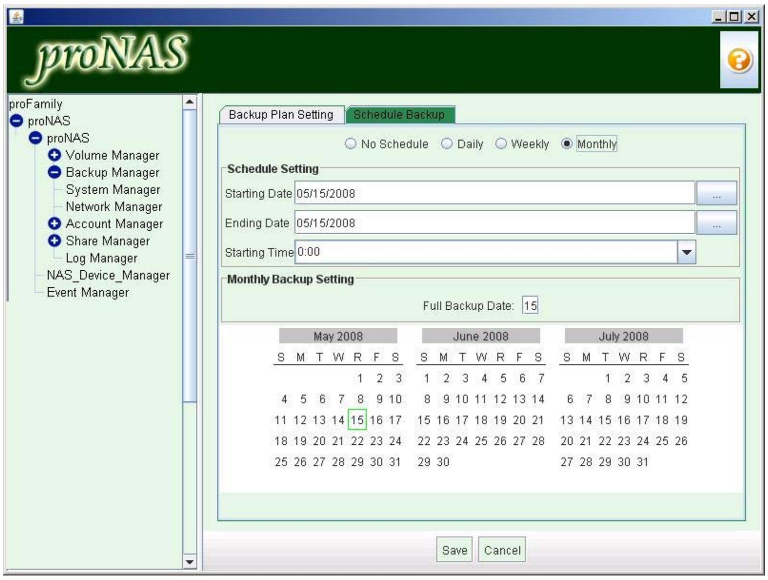
June 2008

S	M	T	W	R	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

July 2008

S	M	T	W	R	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

- **Monthly**: Full backup is the starting point for all data backup. Choose this option to do full backup monthly.



○ No Schedule ○ Daily ○ Weekly ● Monthly

Schedule Setting

Starting Date 05/15/2008

Ending Date 05/15/2008

Starting Time 0:00

Monthly Backup Setting

Full Backup Date: 15

May 2008

S	M	T	W	R	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

June 2008

S	M	T	W	R	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

July 2008

S	M	T	W	R	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

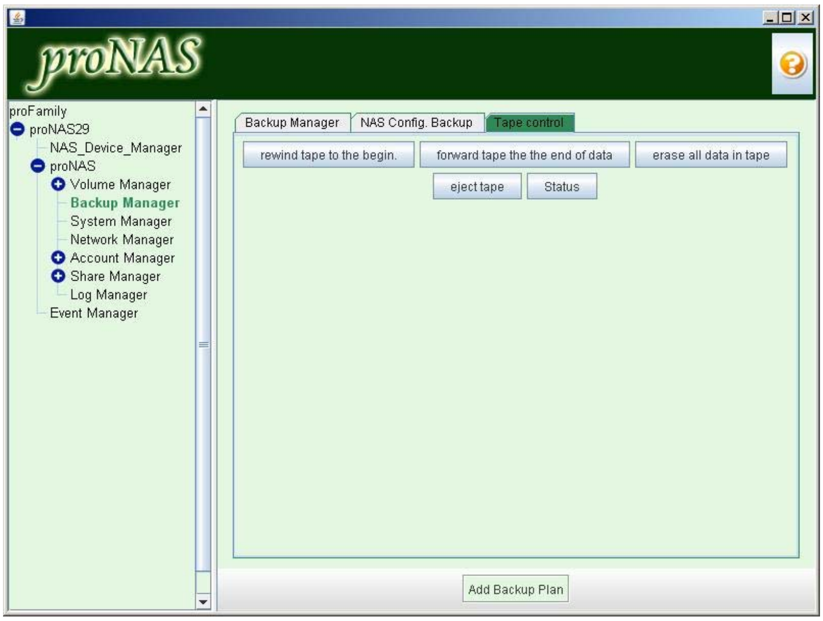
Press "Save" after you completed the settings. Go back to "Backup Plan Setting" tab. You will see the backup plan in the "backup plan list".

If you would like to modify the backup plan, please choose the backup plan in the left tree-node, and press "Edit". If you would like to backup immediately, please press "Backup Now"; or press "Enable schedule backup". System will display schedule enable or disable in "Backup Status" field.

If you would like to restore data from the backup plan, please choose the backup plan in the left tree-node, and go to "Restore" tab, press "Restore" button.

5.6.3 Tape Control

The Tape Control tab allows you to control the tape function when attached to the NAS.



Options:

rewind tape to the begin. – This enables the tape to be rewound to the beginning of the tape.

forward tape to the end of data – This enables the tape to be forwarded to the end of data.

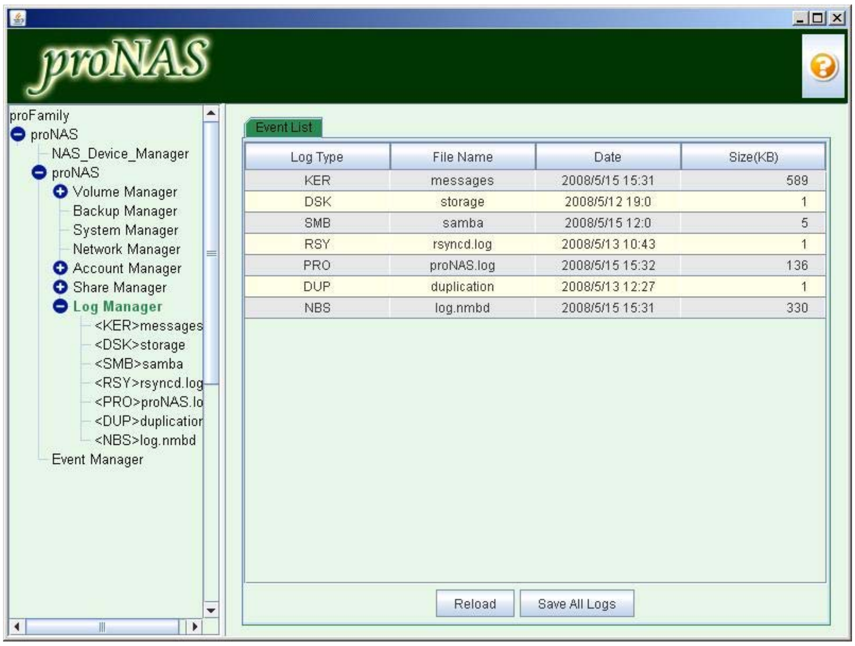
erase all data in tape – This enables the data on the tape to be erased.

eject tape – This enables the tape to be ejected from tape drive.

Status – This shows some information about current status of tape.

5.7 Log Manager

The Log Manager enables you to view the important logs generated by proNAS.



Log Type	File Name	Date	Size(KB)
KER	messages	2008/5/15 15:31	589
DSK	storage	2008/5/12 19:0	1
SMB	samba	2008/5/15 12:0	5
RSY	rsyncd.log	2008/5/13 10:43	1
PRO	proNAS.log	2008/5/15 15:32	136
DUP	duplication	2008/5/13 12:27	1
NBS	log.nmbd	2008/5/15 15:31	330

The Event List tab of the Log Manager lists the log type, file name, date and size (KB). To view the latest log information, please press **"Reload"**.

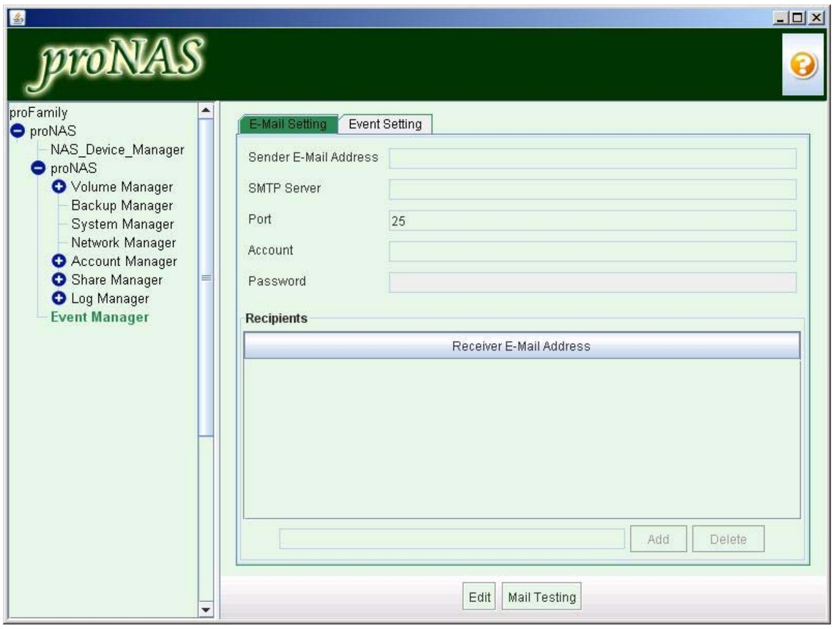
- **KER** - This log contains information about the Linux Kernel service. Its path is /var/log/messages. It can store information of 7 days.
- **SMB** - This log contains information about CIFS and Samba protocol. Its path is /var/log/samba.log
- **DSK** - This log contains information about the changes to volume. Its path is /var/log/storage.log. It can store information of 7 days.
- **SSR** – This contains log information about the SAS RAID card. Its path is /var/log/sasraid.log.
- **NBS** - This log contains information about NetBios protocol service provided by Samba.
- **NWS** - This log contains information about Netware protocol. Its path is /var/log/nws.log
- **BAK** - This log contains the status of Backup Manager.
- **RSY** – This is the log for Rsync service.
- **VRT** - This log contains the status of Veritas.
- **DUP** - This log contains the information of the duplication function.

Save All Logs - Allows you to download the system log files to local folder or destination.

5.8 Event Manager

Event manager is a set of management wherein you can set to receive email notifications or trigger certain commands when a **proNAS**, **proNAS HA** or **NAS Device Manager** event occurs.

5.8.1 E-mail Setting

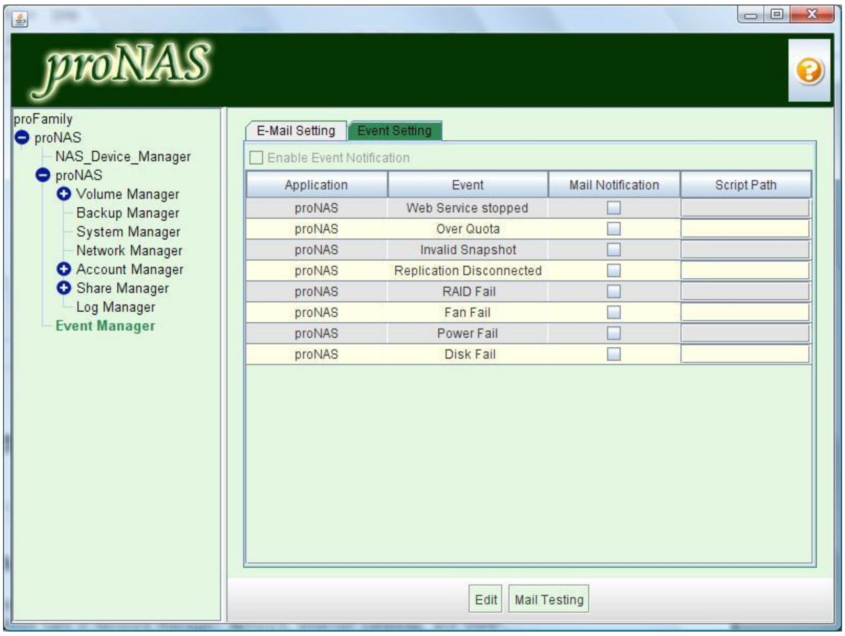


Port 25

Press "Edit" button to edit the following fields:

- **Sender E-mail Address** - Enter the sender's e-mail address.
- **SMTP Server** - Enter the IP address of the SMTP server.
- **Port** - Enter the port number. Default is 25.
- **Accounts** - Enter the SMTP server admin account.
- **Password** - Enter the SMTP server admin password.
- Press "Add" button to insert the e-mail address recipients. You can have multiple receivers.
- If you would like to delete a receiver, select that receiver and then press "Delete".

5.8.2 Event Setting



□ Enable Event Notification

Application	Event	Mail Notification	Script Path
proNAS	Web Service stopped	□	
proNAS	Over Quota	□	
proNAS	Invalid Snapshot	□	
proNAS	Replication Disconnected	□	
proNAS	RAID Fail	□	
proNAS	Fan Fail	□	
proNAS	Power Fail	□	
proNAS	Disk Fail	□	

Press "Edit" button and check the box "Enable Event Notification". Choose the following mail notification. The lists of event options will depend on which service is currently active. By default, all proNAS event will be displayed. Events for proNAS HA or NAS Device Manager will be displayed only after you have started or logon into these services.

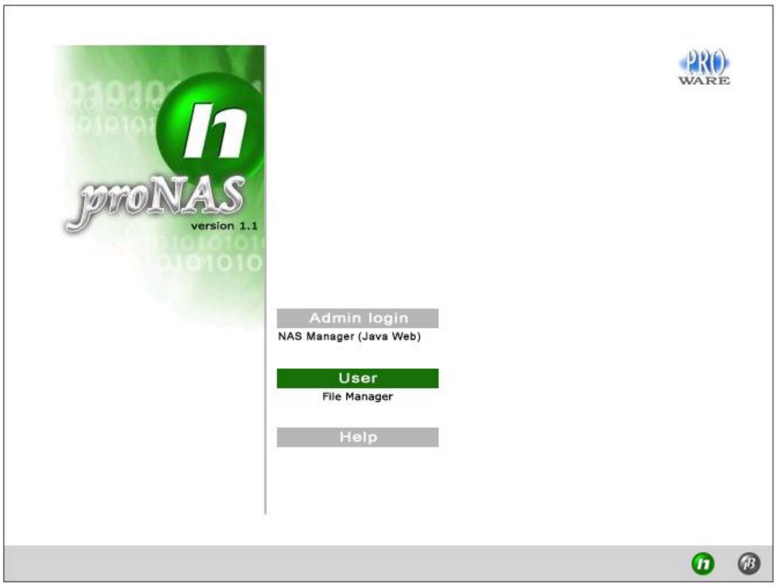
The event options are:

Application	**Event**	**Purpose**
proNAS	Web Service Stopped	Notify if Apache web service is stopped.
proNAS	Logical Volume is Over Quota	Notify if a logical volumes exceeds the given quota. Please check the "Send email when not enough space" for the logical volume.
proNAS	Invalid Snapshot	Notify if a snapshot became invalid.
proNAS	Replication Disconnected	Notify if replication was disconnected.
proNAS	RAID Fail	Notify is a RAID Set or Volume Set fails.
proNAS	Fan Fail	Notify if a fan fails.
proNAS	Power Fail	Notify if a power supply fails.
proNAS	Disk Fail	Notify if a disk drive fails.

Please don't forget to press Enter key after you input the script path.

Chapter 6 File Manager

6.1 Introduction to File Manager



File Manager is a web-base file system for normal account users to do the following actions:

Read a file: User needs the read permission of the folder and the file itself. The file may be opened immediately if the browser knows the corresponding applications that can open it, or the browser will prompt users to save the file in the local computer instead.

Upload a file: User needs the write permission of the folder and the file itself. A browser's upload window will show up and user needs to locate the file from local computer to be uploaded to the current directory.

Create a file: User needs the write permission of the folder. A browser's upload window will show up and user needs to locate the file in local computer.

Delete a file: User needs the write permission of the folder and the file itself.

Rename a file: Same as above. User needs to give the new name of a file.

Change Password: If user needs to change password, please select this function.

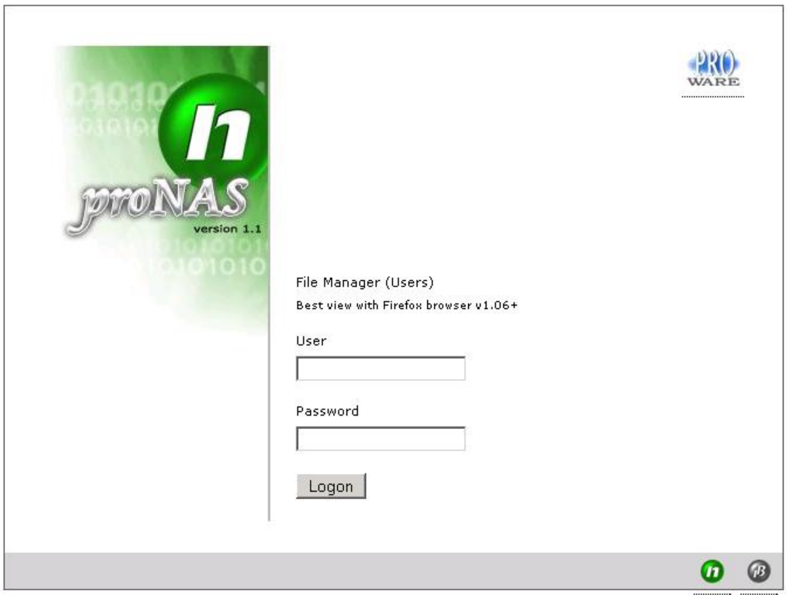
Access Right (Change the ACL of a file or sub-folder): User needs to be the creator or the owner of the share folder. A user is the creator of a file or folder if user creates it.

The owner of a share folder can grant the access permission of a share to other accounts or access groups. User also can manage the ACL of all the files and sub-folders under the share.

The function of access right is for share owner to do more detail management for the users accessing the shares. Share owner can increase or delete the access right of users or groups in addition to the setting of administrator in proNAS GUI. Furthermore, share owner can manage the detail access right of the subfolders.

6.2 Logon to File Manager

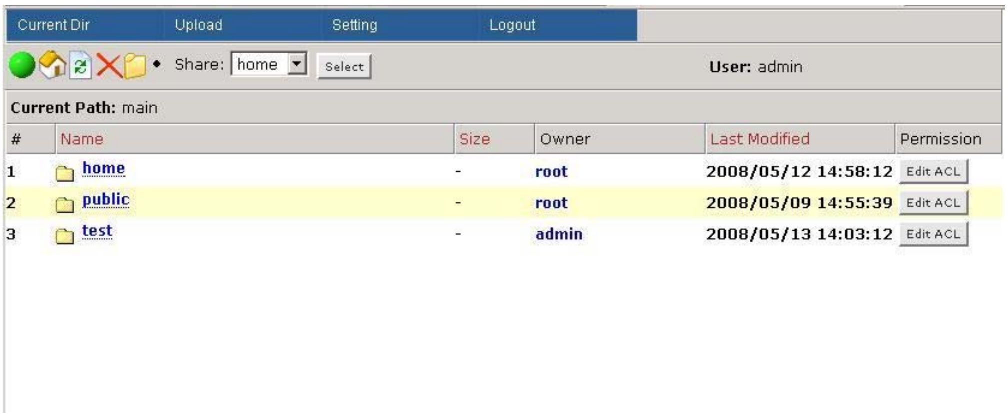
Enter the username and password to pass authentication.



File Manager (Users)

Best view with Firefox browser v1.06+

The first Screen of file Manager will display and help users to understand the possible options and to perform file management. There are 4 Main Menu in the File Manager screen: CurrentDir, Upload, Setting, and Logout. There are also short-cut icons below the main menu, like Main, Home, Reload Page, Delete Current Folder, and Create New Folder.



User: admin

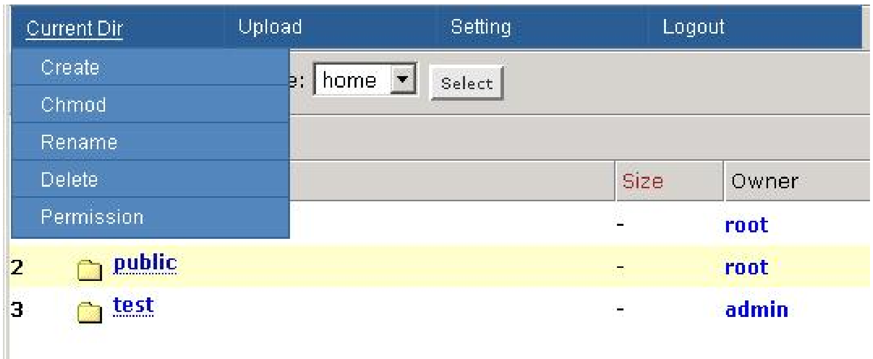
Current Path: main

#	Name	Size	Owner	Last Modified	Permission
1	home	-	root	2008/05/12 14:58:12	Edit ACL
2	public	-	root	2008/05/09 14:55:39	Edit ACL
3	test	-	admin	2008/05/13 14:03:12	Edit ACL

6.3 Directory and Upload Function

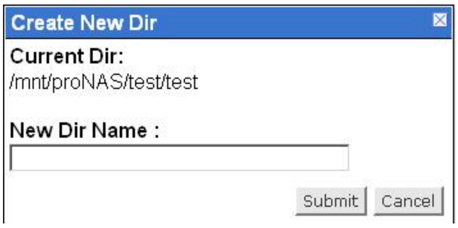
NOTE: Operations in the main Share folder, such as changing ACL or deleting the share itself, is not permitted. This must be done in Share Manager in proNAS GUI.

Current Dir – Shows possible options that can be done in the current directory.



		Size	Owner
		-	root
2	public	-	root
3	test	-	admin

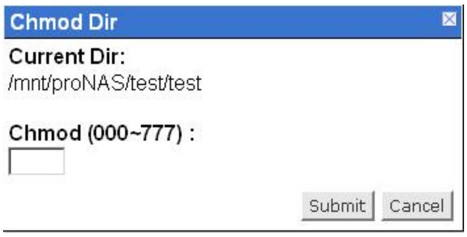
- ♦ Create – Allows user to create a new directory.



Current Dir:
/mnt/proNAS/test/test

New Dir Name :

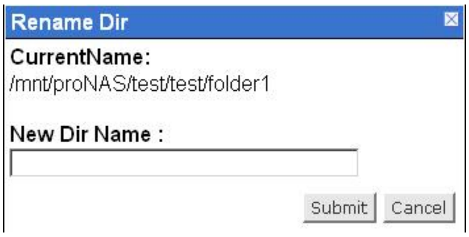
- ♦ Chmod – Allows user to change the file access permission on the current directory.



Current Dir:
/mnt/proNAS/test/test

Chmod (000~777) :

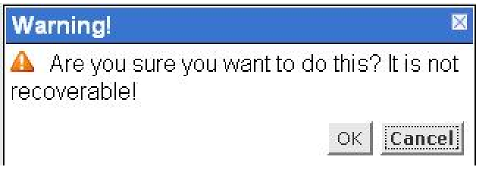
- ♦ Rename – Allows user to rename the current directory.



CurrentName:
/mnt/proNAS/test/test/folder1

New Dir Name :

- Delete – Allows a user to delete the current directory.

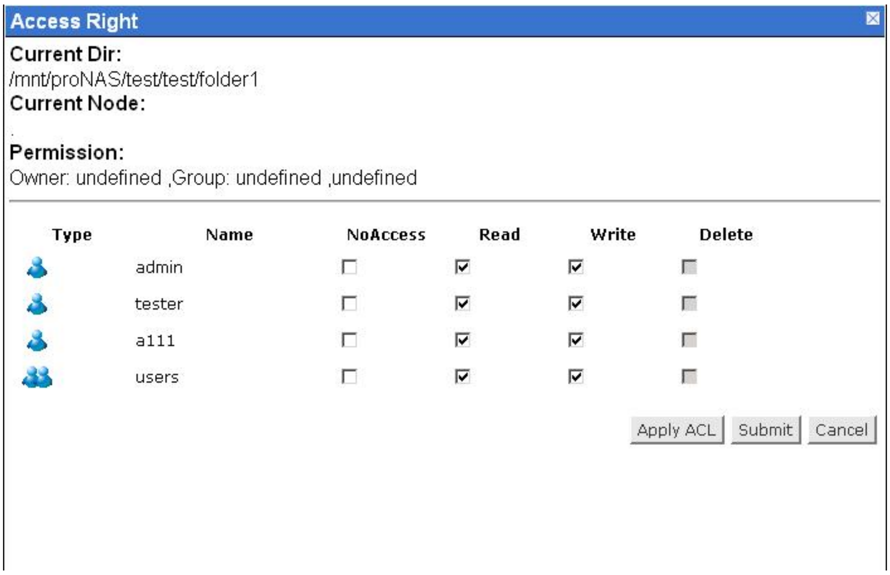


Warning! ☒

⚠ Are you sure you want to do this? It is not recoverable!

OK | Cancel

- Permission – Allows user to change the Access Rights of different users on the current directory.



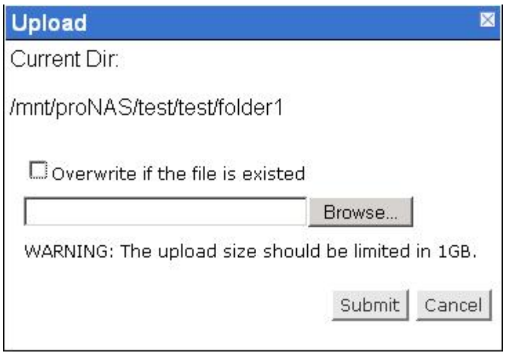
Access Right ☒

Current Dir:
/mnt/proNAS/test/test/folder1
Current Node:
.
Permission:
Owner: undefined ,Group: undefined ,undefined

Type	Name	NoAccess	Read	Write	Delete
👤	admin	☐	☑	☑	☐
👤	tester	☐	☑	☑	☐
👤	a111	☐	☑	☑	☐
👥	users	☐	☑	☑	☐

Apply ACL | Submit | Cancel

Upload – An option used to upload a local file into the current directory. Use the “Browse” button then select the file to upload.



Upload ☒

Current Dir:

/mnt/proNAS/test/test/folder1

☐ Overwrite if the file is existed

Browse...

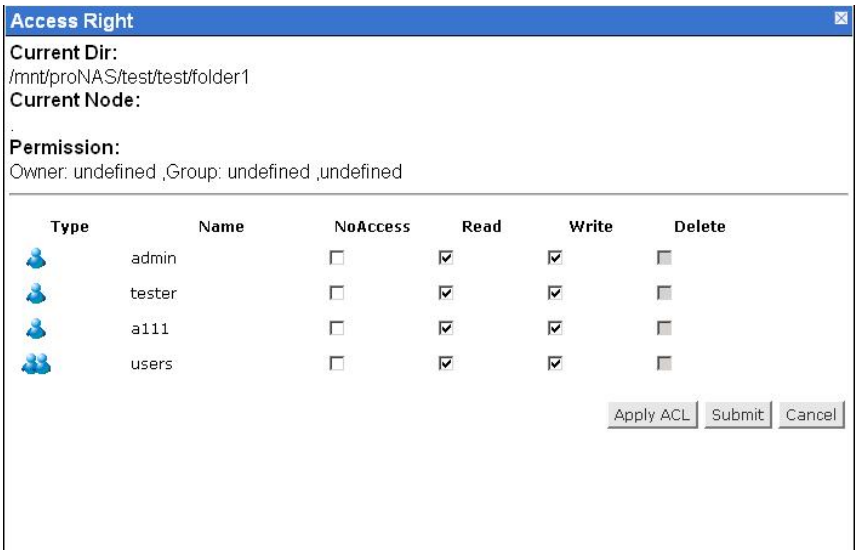
WARNING: The upload size should be limited in 1GB.

Submit | Cancel

⚠ **WARNING! The file size to upload should not be greater than 1GB.**

6.4 User Access Right and Group Access Right

A user who is the owner of the share can grant access permissions to other users or groups listed in the Permission list.



Access Right

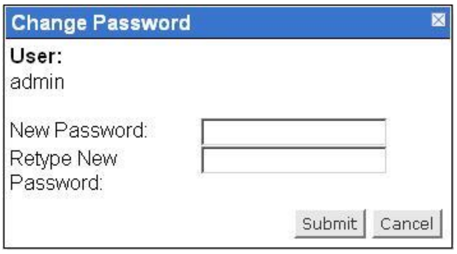
Current Dir:
/mnt/proNAS/test/test/folder1
Current Node:
.
Permission:
Owner: undefined ,Group: undefined ,undefined

Type	Name	NoAccess	Read	Write	Delete
👤	admin	□	☑	☑	□
👤	tester	□	☑	☑	□
👤	a111	□	☑	☑	□
👥	users	□	☑	☑	□

After changing the Access Rights, click the "Submit" button. The ACL will be saved and updated only in the current directory or sub-folder. To update other directories or sub-folders below the current directory, use the "Apply ACL" button. This will propagate the current ACL to the ACL off all files and sub-folders below. To cancel any changes, click the "Cancel" button.

6.5 Change Password and Logout

Setting – Allows a use to change his/her password.



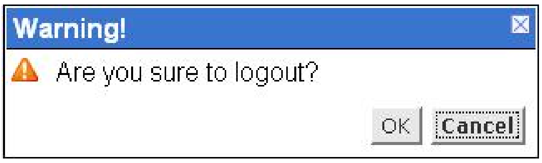
Change Password

User:
admin

New Password:
Retype New Password:

NOTE: The password must be at least 6 characters in length.

Logout - Allows a user to logout from the current session of File Manager.



Warning!

Are you sure to logout?

Chapter 7 proBackup

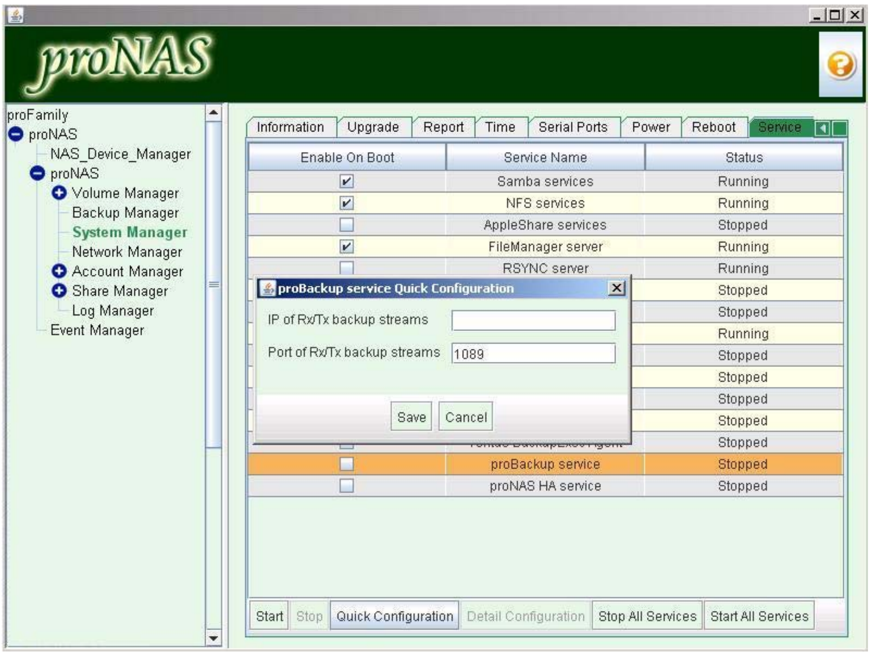
7.1 Introduction to proBackup

proBackup provides end users a friendly Java GUI that makes versatile backup functions available to general users. They can easily backup and restore their files to and from proBackup storage device, and they do not need to install proprietary software in their machines. It is also simple to setup a proBackup storage for a company or an organization, even for non-IT-pro person.

7.2 Administrator Logon

The administrator account, admin, can login to proBackup. In proNAS Manager, admin can also assign other privileged users to become member of the proBackup group. Only admin and members of the proBackup group can login to proBackup and perform proBackup functions.

Before admin or proBackup user can login to proBackup Java GUI, the proBackup service must be started in Service tab of System Manager. In Quick Configuration, setup the **"IP of Rx/Tx backup streams**" to the **proNAS IP address** that will be used as the channel for proBackup. The **"Port of Rx/Tx backup streams"** is set to 1089 by default. If this port is already used, assign another port.



Enable On Boot	Service Name	Status
☑	Samba services	Running
☑	NFS services	Running
□	AppleShare services	Stopped
☑	FileManager server	Running
□	RSYNC server	Running
		Stopped
		Stopped
		Running
		Stopped
		Stopped
		Stopped
		Stopped
□	Veritas BackupExec Agent	Stopped
□	proBackup service	Stopped
□	proNAS HA service	Stopped

proBackup service Quick Configuration

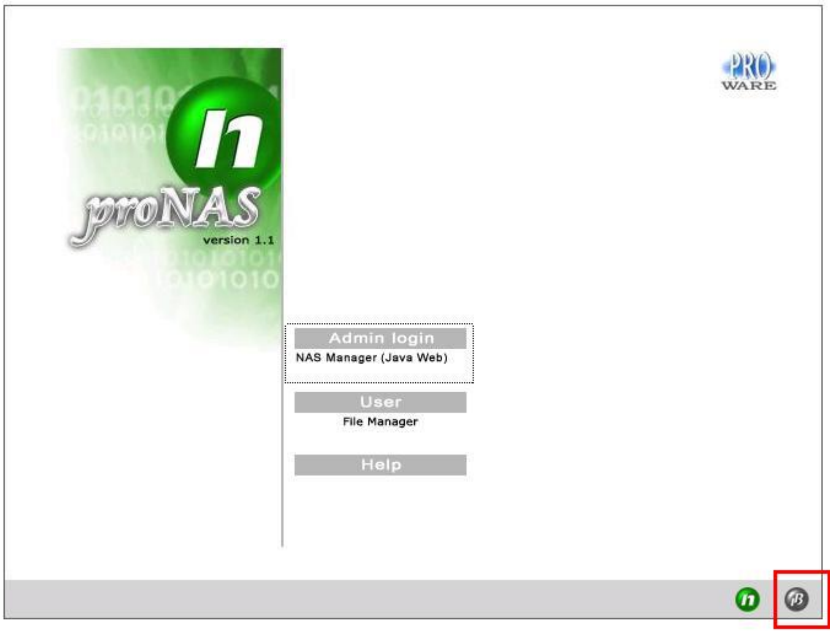
IP of Rx/Tx backup streams:

Port of Rx/Tx backup streams: 1089

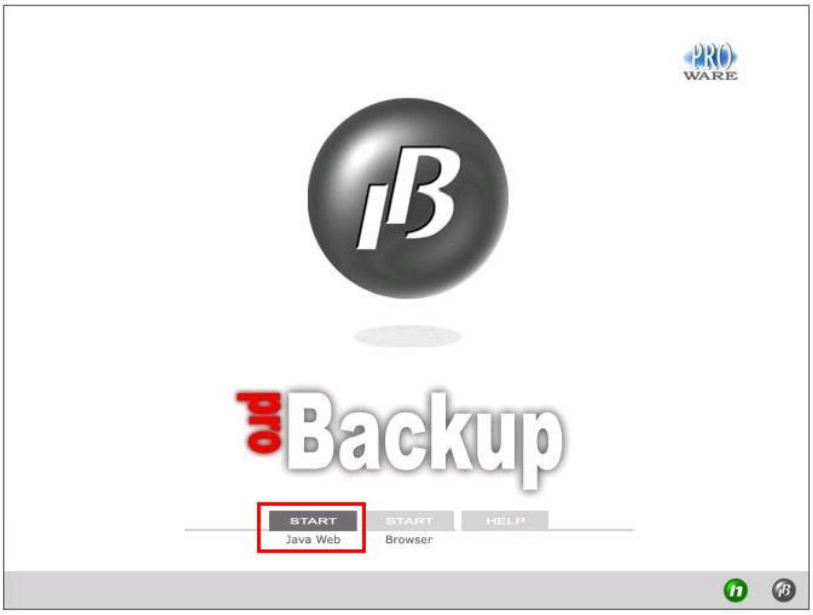
Save | Cancel

After setting the Quick Configuration options, start the proBackup service. When the proBackup service is in “Running” status, login to proBackup Java GUI can be done. The default Logical Volumes **proBackup Device** and **proBackup Extended Device** will also be created.

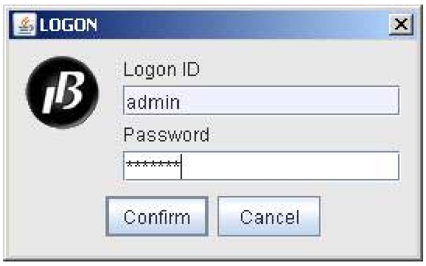
To login to proBackup java GUI, open web browser then type the proNAS IP address. Click the proBackup icon on the lower right side of the page.



The proBackup page will be displayed. Click “Start Java Web”.



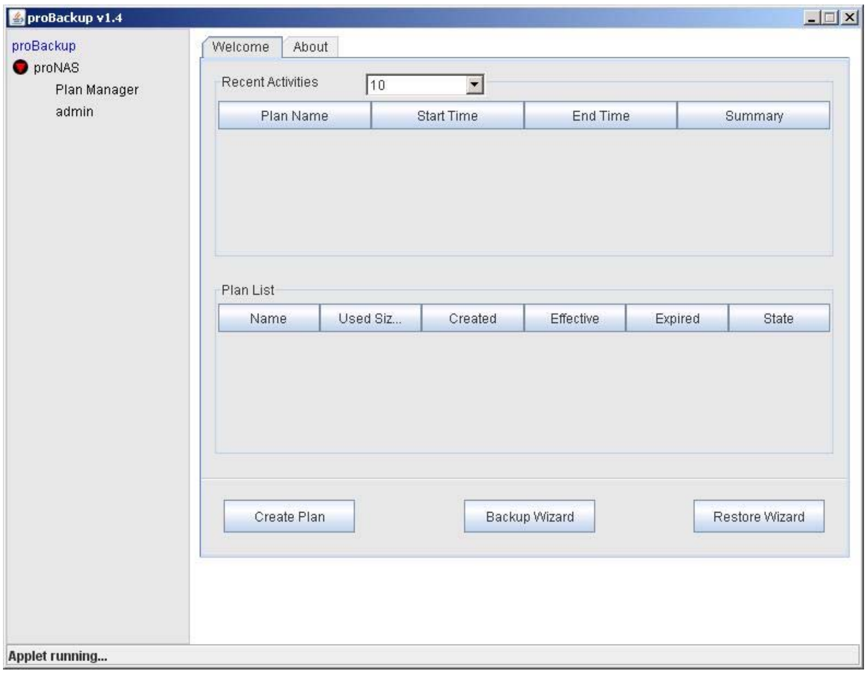
Enter the login account and password.



NOTE: All the backups of an account are lost forever if it is deleted. Please make sure such action before doing it.

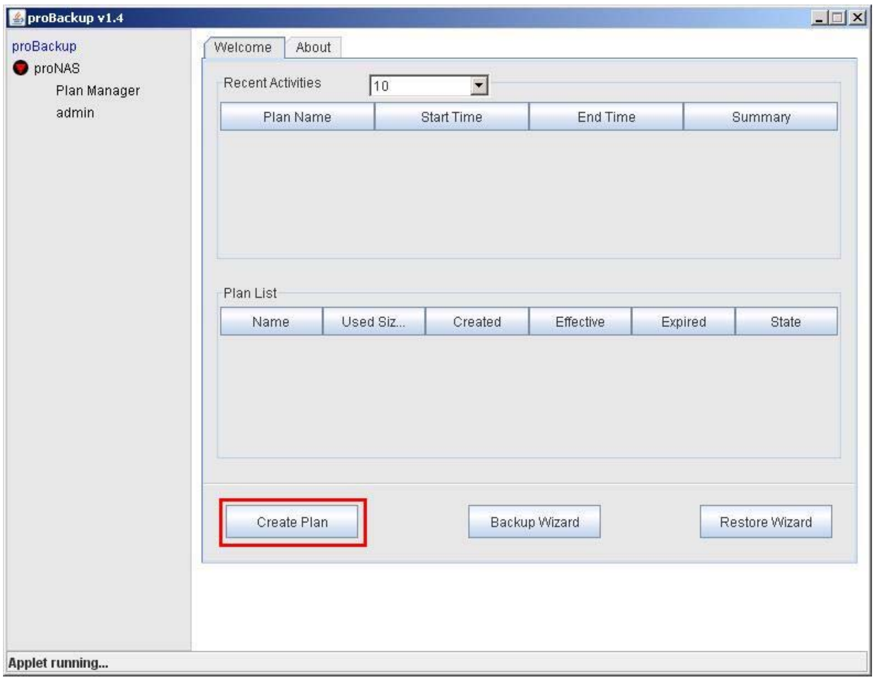
NOTE: It is advised that only the organization privilege persons can assume the role of administrator since it can restore all others' data, which may contain sensitive information.

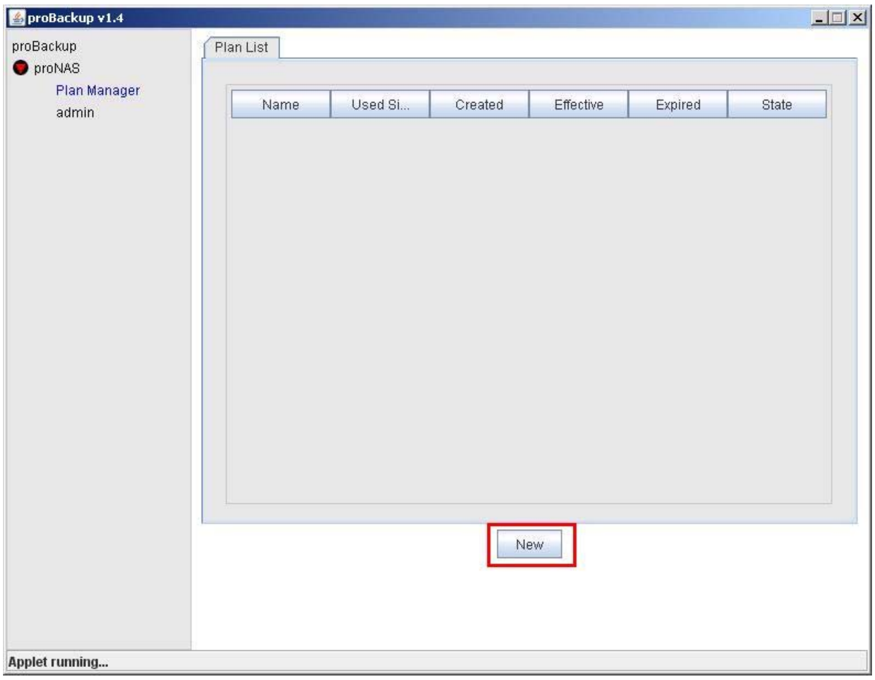
The proBackup Java GUI Welcome screen will be displayed. You can view the recent proBackup operations and existing backup plans in the Welcome screen. To learn about proBackup release version, click the About tab.



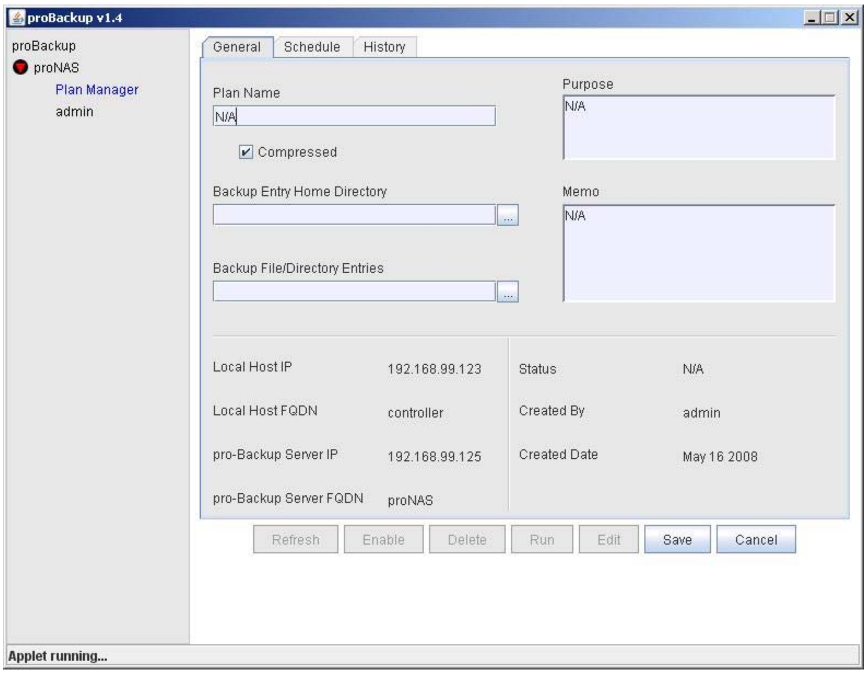
7.3 Create Backup Plan

To create backup plan, either click the "Create Plan" button in the proBackup main screen or click the "New" button in Plan Manager.





The General tab of Plan Manager will be displayed. Fill in the required fields. Some information about Local Host and proBackup Server are also shown.



Plan Name: N/A

☑ Compressed

Backup Entry Home Directory:

Backup File/Directory Entries:

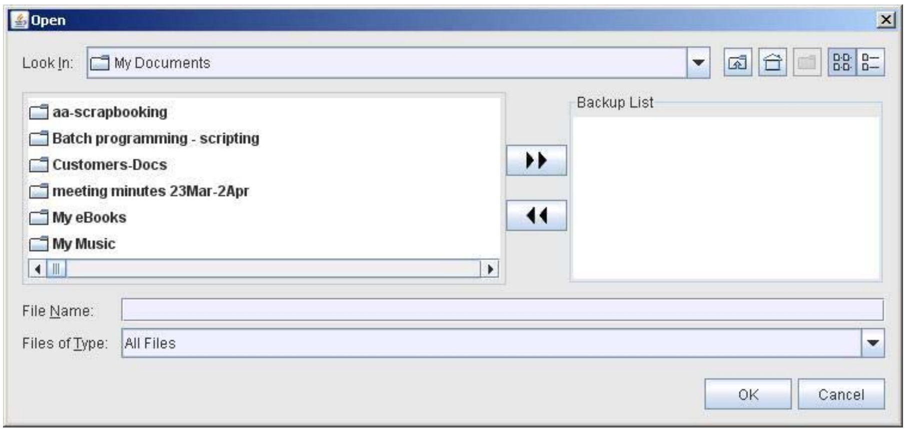
Purpose: N/A

Memo: N/A

Local Host IP	192.168.99.123	Status	N/A
Local Host FQDN	controller	Created By	admin
pro-Backup Server IP	192.168.99.125	Created Date	May 16 2008
pro-Backup Server FQDN	proNAS		

The Configuration options:

- **Plane Name** – Enter the backup plan name.
- **Compressed** – If checked, the backup will be in compressed format.
- **Backup Entry Home Directory** – Click the "…" button then select the directory when data will be backed up.
- **Backup File / Directory Entries** – Click the "…" button. Select the files and/or directories to be backed up then click ">>" button to add them to the backup list. Click "OK" to go back to General tab.



Look In: My Documents

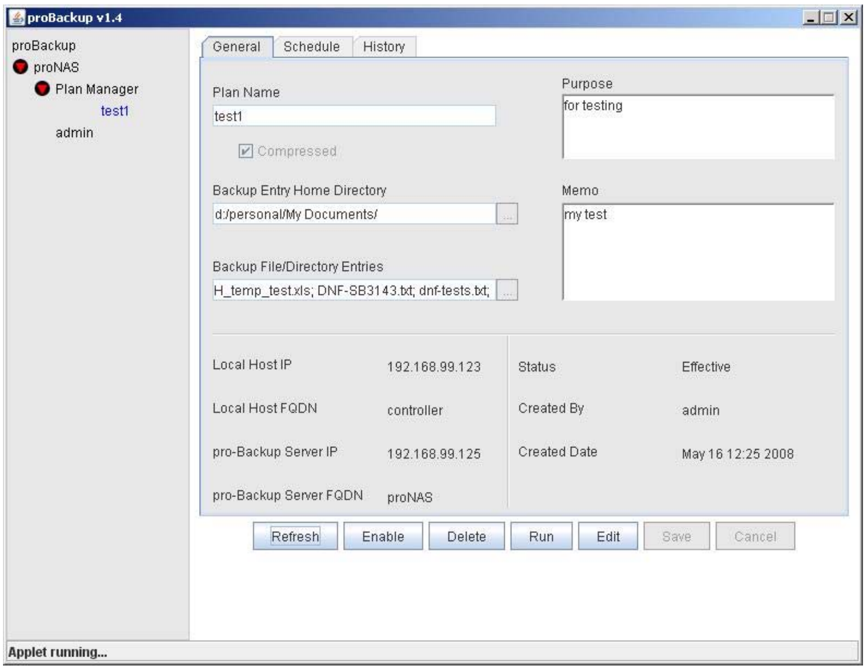
aa-scrapbooking
Batch programming - scripting
Customers-Docs
meeting minutes 23Mar-2Apr
My eBooks
My Music

File Name:

Files of Type: All Files

- **Purpose** – Enter additional information in this optional field.
- **Memo** – Enter additional information in this optional field.

After completing the necessary information, click "Save" button. The Backup Plan will be saved.



Plan Name: test1

☑ Compressed

Purpose: for testing

Backup Entry Home Directory: d:/personal/My Documents/

Memo: my test

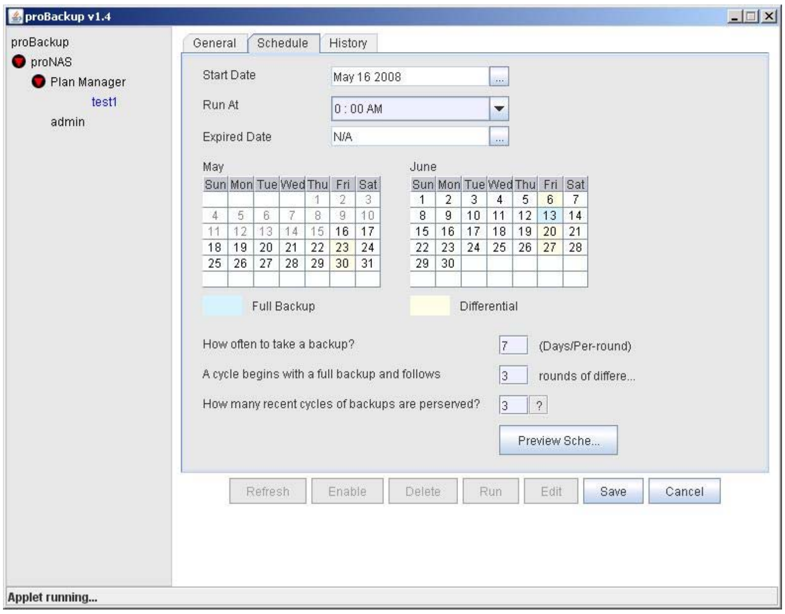
Backup File/Directory Entries: H_temp_test.xls; DNF-SB3143.txt; dnf-tests.txt;

Local Host IP	192.168.99.123	Status	Effective
Local Host FQDN	controller	Created By	admin
pro-Backup Server IP	192.168.99.125	Created Date	May 16 12:25 2008
pro-Backup Server FQDN	proNAS		

Function buttons in the General tab.

- **Refresh** – Refresh the information about the current backup plan.
- **Enable** – Activates the backup plan schedule. When enabled, a "**Disable**" button will appear which can be used to deactivate the backup schedule.
- **Delete** – Deletes the current backup plan.
- **Run** – Execute the backup plan immediately.
- **Edit** – Use this to change settings in the backup plan.

To add schedule in the Backup Plan, click the “Edit” button then select Schedule tab. Configure the Schedule options then click “Save” when done.



Start Date May 16 2008

Run At 0 : 00 AM

Expired Date N/A

May

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

June

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Full Backup

Differential

How often to take a backup? 7 (Days/Per-round)

A cycle begins with a full backup and follows 3 rounds of differe...

How many recent cycles of backups are perserved? 3 ?

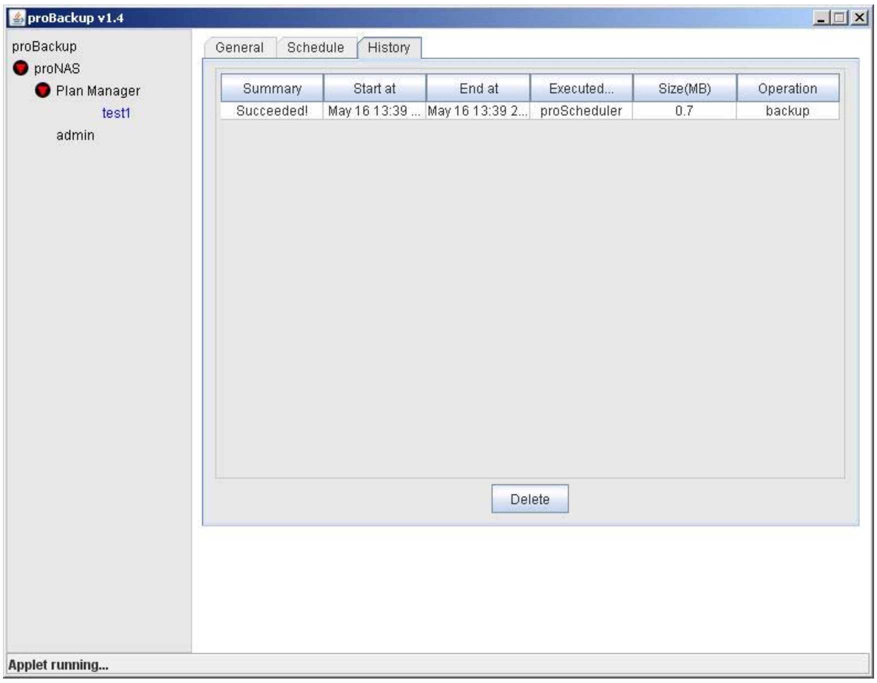
Schedule options:

- **Start Date** – The starting date when the backup will be done. This usually defaults to the current date. Click the “…” button. A calendar will be displayed. To change the Start Date, select a new date in the calendar.
- **Run At** – The preferred time to run the backup. To change the Run At time, click the pull-down arrow then select the preferred time.
- **Expired Date** – The ending date for the backup. To change the Expired Date, click the “…” button then select in the calendar the preferred last date of backup.
- **How often to take a backup? (Days/Round)** – The number of days that will pass before a differential backup will be done.
- **A cycle begins with a full backup and follows rounds of differential backup** – Enter the number of differential backups that will be made before starting a new full backup.
- **How many recent cycles of backups are preserved?** – Enter a number which is the total number of backup cycles that will be preserved. A backup cycle starts with a full backup and ends with the last differential backup before the next full backup. When the number of cycles in a schedule has been reached and a new cycle is started, the oldest backup cycle will be automatically removed.
- **Preview Schedule** – Click this button to update the calendar schedule.

  - **Full Backup** – archival backup; all files are copied to a backup storage device
  - **Differential Backup** – backup only the data files that have been modified since the last full backup

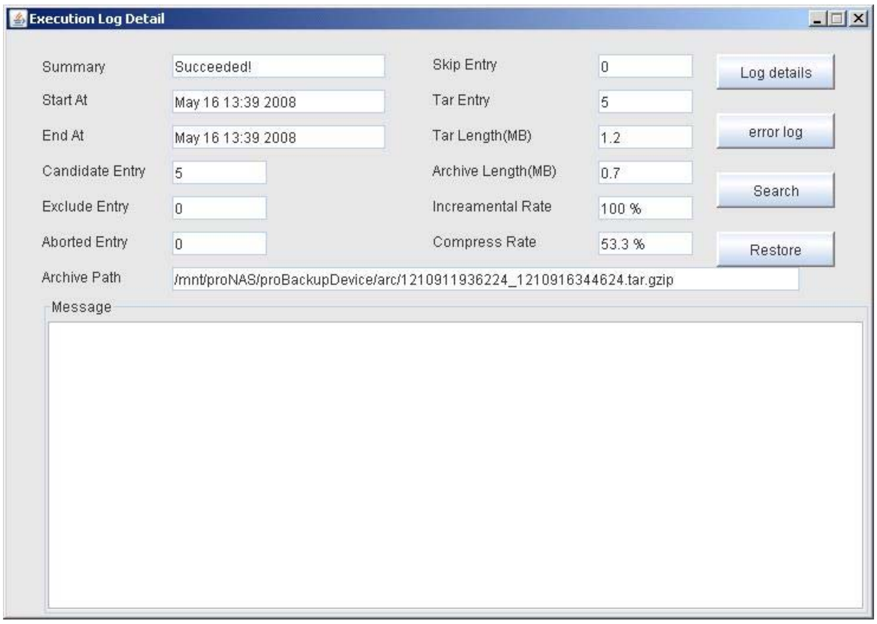
Click “Save” to update the schedule settings. Then click “Enable” to activate the backup schedule.

The History tab shows a log or list of operations that have happened in proBackup such as backup or restore operation. To delete an entry in the history list, select the item in the list and click “Delete”.



Summary	Start at	End at	Executed...	Size(MB)	Operation
Succeeded!	May 16 13:39 ...	May 16 13:39 2...	proScheduler	0.7	backup

To view detailed information about the backup, double-click the item from the History tab.

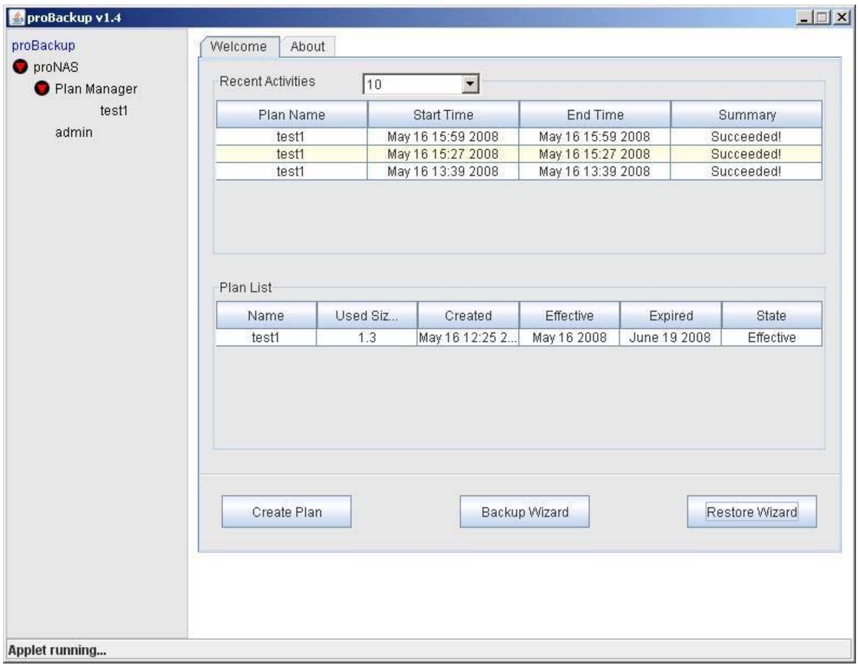


Summary	Succeeded!	Skip Entry	0
Start At	May 16 13:39 2008	Tar Entry	5
End At	May 16 13:39 2008	Tar Length(MB)	1.2
Candidate Entry	5	Archive Length(MB)	0.7
Exclude Entry	0	Increamental Rate	100 %
Aborted Entry	0	Compress Rate	53.3 %

Archive Path: /mnt/proNAS/proBackupDevice/arc/1210911936224_1210916344624.tar.gzip

“Log details” is used to display detailed information about the execution process.
“Error log” will display errors that happened during the execution process.
“Search” will allow you to search for a string currently displayed in the Message screen.
“Restore” will allow you to restore a backup.

Another alternative to do backup or restore is to use the Backup Wizard and the Restore Wizard. Click proBackup in the left tree node. The Welcome screen will be displayed where the Backup Wizard and Restore Wizard can be used.



Recent Activities 10

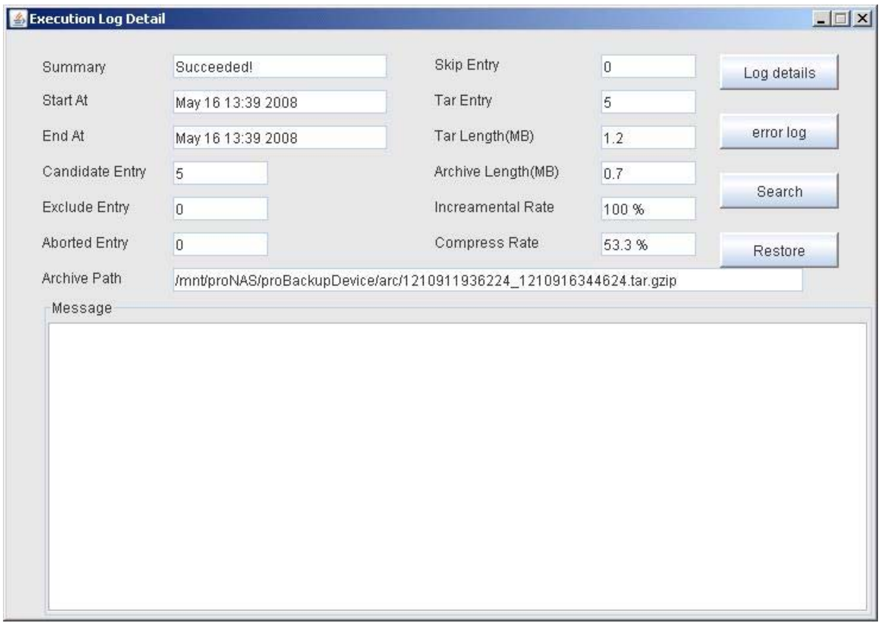
Plan Name	Start Time	End Time	Summary
test1	May 16 15:59 2008	May 16 15:59 2008	Succeeded!
test1	May 16 15:27 2008	May 16 15:27 2008	Succeeded!
test1	May 16 13:39 2008	May 16 13:39 2008	Succeeded!

Plan List

Name	Used Siz...	Created	Effective	Expired	State
test1	1.3	May 16 12:25 2...	May 16 2008	June 19 2008	Effective

7.4 Restore Backup

To restore a backup, double-click the backup item from the History tab. The Execution Log Detail window will appear.



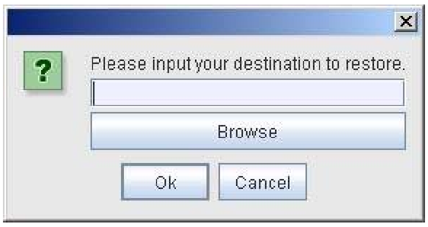
Execution Log Detail

Summary	Succeeded!	Skip Entry	0	Log details
Start At	May 16 13:39 2008	Tar Entry	5	
End At	May 16 13:39 2008	Tar Length(MB)	1.2	error log
Candidate Entry	5	Archive Length(MB)	0.7	
Exclude Entry	0	Increamental Rate	100 %	Search
Aborted Entry	0	Compress Rate	53.3 %	Restore

Archive Path /mnt/proNAS/proBackupDevice/arc/1210911936224_1210916344624.tar.gzip

Message

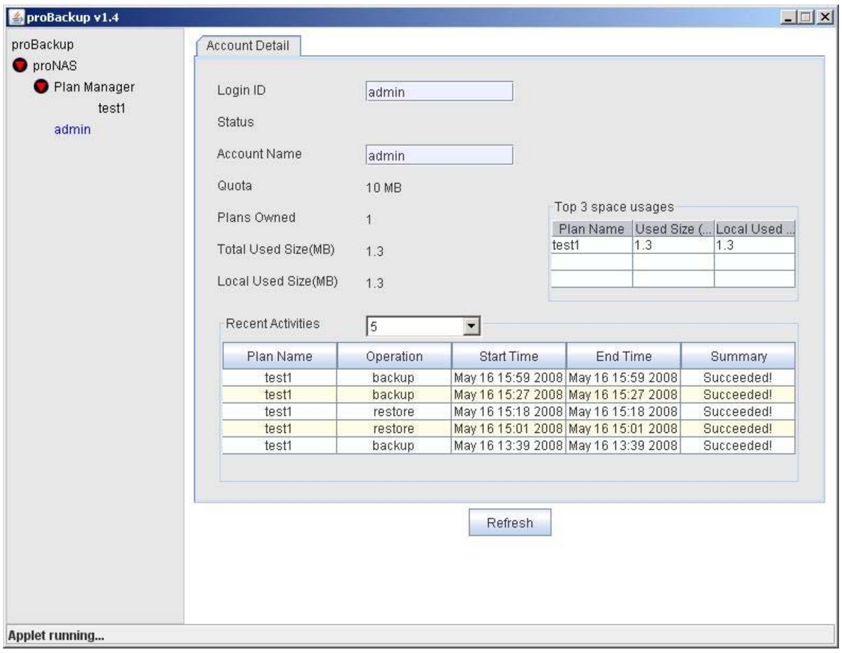
Click "Restore". Then input the destination where the data will be restored. Or click the "Browse" button then select the destination directory or folder where data will be restored. Click "Ok" to start the restore process.



Please input your destination to restore.

7.5 Account Detail

Under Plan Manager, click the account name to view information about the account.



Login ID admin

Status

Account Name admin

Quota 10 MB

Plans Owned 1

Total Used Size(MB) 1.3

Local Used Size(MB) 1.3

Top 3 space usages

Plan Name	Used Size (...	Local Used ...
test1	1.3	1.3

Recent Activities 5

Plan Name	Operation	Start Time	End Time	Summary
test1	backup	May 16 15:59 2008	May 16 15:59 2008	Succeeded!
test1	backup	May 16 15:27 2008	May 16 15:27 2008	Succeeded!
test1	restore	May 16 15:18 2008	May 16 15:18 2008	Succeeded!
test1	restore	May 16 15:01 2008	May 16 15:01 2008	Succeeded!
test1	backup	May 16 13:39 2008	May 16 13:39 2008	Succeeded!

Chapter 8 proNAS HA (Optional Function)

8.1 Introduction to proNAS HA

proNAS HA (High Availability) provides solution for business continuity with automatic failover which ensures that should a critical server become unavailable - due to failure or maintenance-related downtime — a replica will immediately provide all services in its place without the need for time-consuming manual procedures.

The core processes of ProNAS HA are implemented as two mutual-guarded fail-safe proNAS services. They can be manipulated by accessing the Services tab in the proNAS System Manager node. The dual service architecture of ProNAS HA prevents ProNAS HA from being the single-point-of-failure of the server cluster.

When a server is down or unavailable, ProNAS HA switches the critical operations of that server over to the peer server automatically. The switch over procedure can also be triggered manually to handle scheduled downtime more gracefully and user transparently. ProNAS HA can be manually instructed to switch over the critical operations of a server to the peer server. Users can then perform upgrade, replacement, or maintenance to the hardware and software of that proNAS server. The critical operations of a server can be configured as auto-switch back. After those critical operations were taken over by the peer server, ProNAS HA can switch them back to their original active server when the active server becomes available again. Auto-switch back ensures that the original load distribution between the two servers will be resumed immediately when possible.

proNAS HA provides:

- Manual or auto-triggered failover to a standby server.
- Supports manual or automatic failover back to the original server when ready
- Real-time replication minimizes potential data loss

8.2 Getting Started with proNAS HA

Before Configuring High Availability

Before attempting to configure two proNAS HA as a High Availability pair, check the following requirements:

1. Each proNAS server box must have a different and unique hostname. (It is highly recommended to use the same NAS model.)
2. Each proNAS box must have at least two static IP addresses.
3. Must have a reliable heartbeat, private net Ethernet is required, serial RS232 is optional.
4. proNAS HA services must be started in both proNAS servers.
5. The maximum number of logical volumes that can be created under HA is 32.
6. proNAS HA does not support logical volumes larger than 2TB. Users can create and extend volumes larger than 2TB but this cannot be used in proNAS HA.
7. Changing hostname and IP addresses when proNAS HA is running is not allowed.
8. Snapshot function is disabled under HA.
9. Be sure there are no scheduled snapshot task enabled either on each proNAS box.

Setting up a private network:

Private net is a communication channel between the two proNAS box through which they exchange information about their states (*heartbeats*). proNAS supports two private network, TCP/IP Socket and RS232 Serial Port.
To setup TCP/IP private net: Connect a dedicated network into Ethernet1 adapter. You may use a crossover cable. Ethernet0 serves as your public net.
To setup RS232 Serial Port private net: Connect a serial cable to either Com1 or Com2 for both proNAS box then configure it under the "Serial Port" tab on System Manager.

NOTE: It is recommended to use both TCP/IP and RS-232 for your private net. Private net IP will be used for replication and RS-232 for heartbeat.

NOTE: Some proNAS models have eth0 Fast Ethernet port. In order to have faster access to your proNAS, use the Gigabit Ethernet port (eth1, if eth0 is Fast Ethernet) as your public net; that is where the users access your proNAS. Then use eth2 as your Private Net.

8.2.1 Hardware Aspect

Active server: proNAS HA server that performs cluster-protected operations.

Backup (Standby) server: proNAS HA server that can takeover the critical operations of an active server when the active server is down or unavailable.

Private net: Private net is a dedicated channel for servers to exchange their operating status (i.e., heartbeat message).

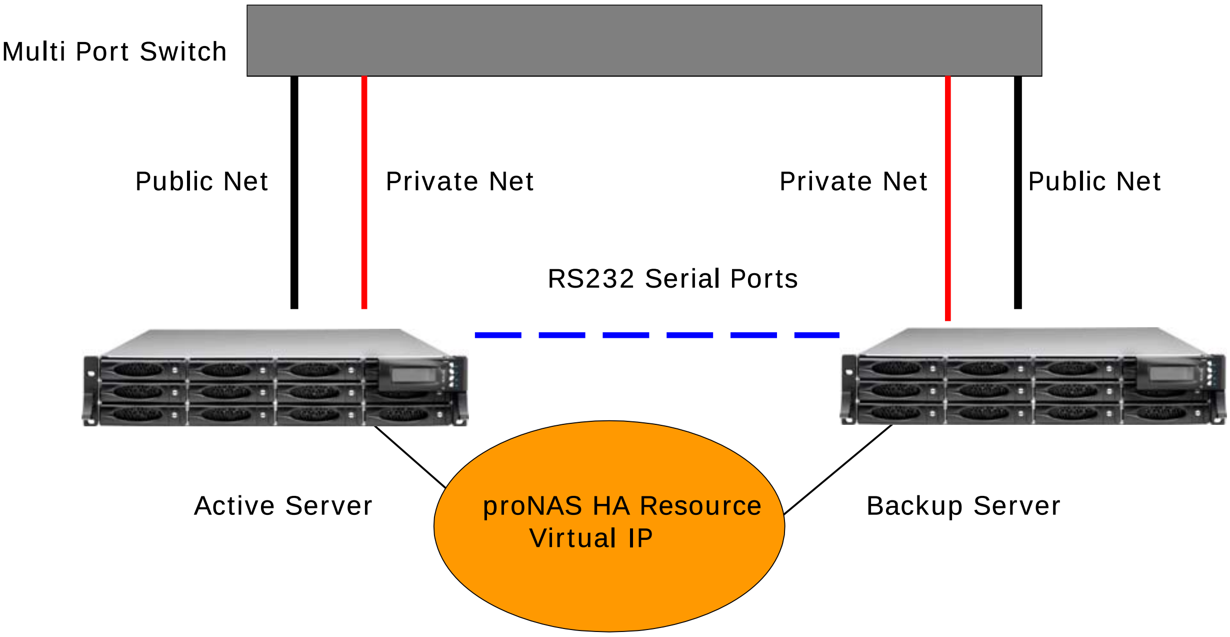
Types of Private Net Available:

- **TCP/IP socket:** Ethernet network running TCP/IP protocol. Each server must install a dedicated IP to attach to the private net.
- **RS-232 serial port:** One free serial port per server. A null modem cable must be installed to connect the serial ports of the two servers.

Public net: Public net is the paths for networked clients to access cluster- protected resources.

Network Configuration for High Availability Pair

The following diagram illustrates the network configuration for a High Availability pair:



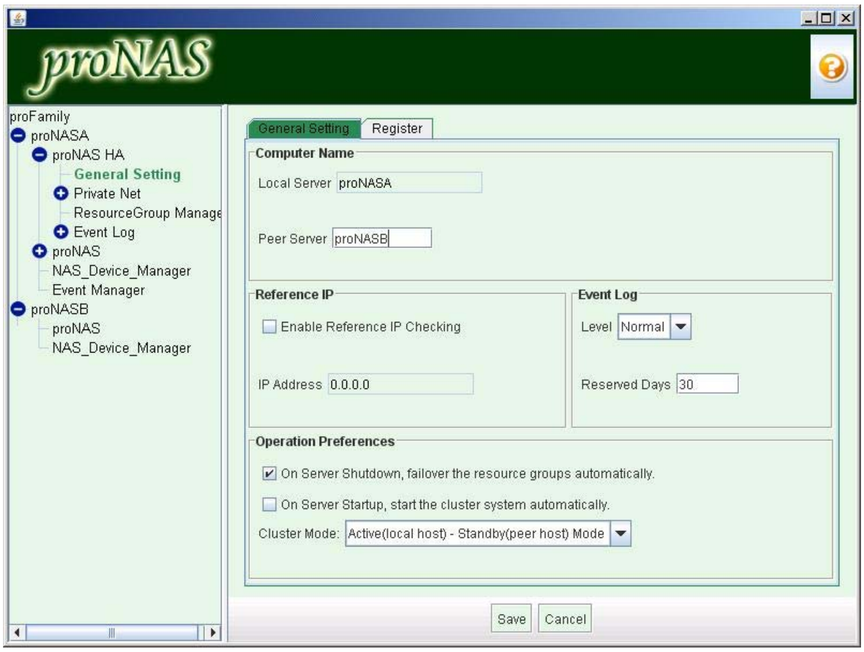
8.2.2 Procedure for Setting Up proNAS HA

Setting up a server cluster:

Below are the basic steps in setting up a server cluster:

1. Configure the hostname for both proNAS servers (must be unique).
2. Configure two static IP addresses for each proNAS server.
3. Set up private net. At least the private net IP must be configured to start cluster.
4. Start proNAS HA service for both proNAS servers. You may do this under System Manager then Services tab, highlight proNAS HA service then click Start. proNAS HA node will then appear on the left tree after it starts successfully.
5. On the designated Active Server, go to proNAS HA->"General Settings".
6. On the "General Setting" tab, click "Edit" button. Input the Peer Server hostname then select "**Active (local-host) – Standby (peer host) Mode**" under the Cluster mode. Click "Save".

NOTE: The Cluster Mode of Backup Server must be configured as “Standby(local host) – Active(peer-host) Mode” (see Step 10).



Computer Name

Local Server proNASA

Peer Server proNASB

Reference IP

☐ Enable Reference IP Checking

IP Address 0.0.0.0

Event Log

Level Normal

Reserved Days 30

Operation Preferences

☑ On Server Shutdown, failover the resource groups automatically.

☐ On Server Startup, start the cluster system automatically.

Cluster Mode: Active(local host) - Standby(peer host) Mode

Other configuration options:

Computer Name:

Local Server: The hostname of the Active or Primary server

Peer Server: The hostname of the Backup or Secondary server

Reference IP:

Enable Reference IP Checking – Select this option to enable reference IP checking. A Reference IP is an IP that the proNAS HA service will check when the heartbeat channel(s) between the two servers are lost. The IP of a router or any network device which is always online can be used as a Reference IP.

IP Address – Enter the IP address of the Reference IP to check the availability of the servers.

Event Log:

Level – Select the type of logging that will be used for proNAS HA service. Default is Normal which shows operation processes. Other option is Trace, which shows operation and traceable processes.

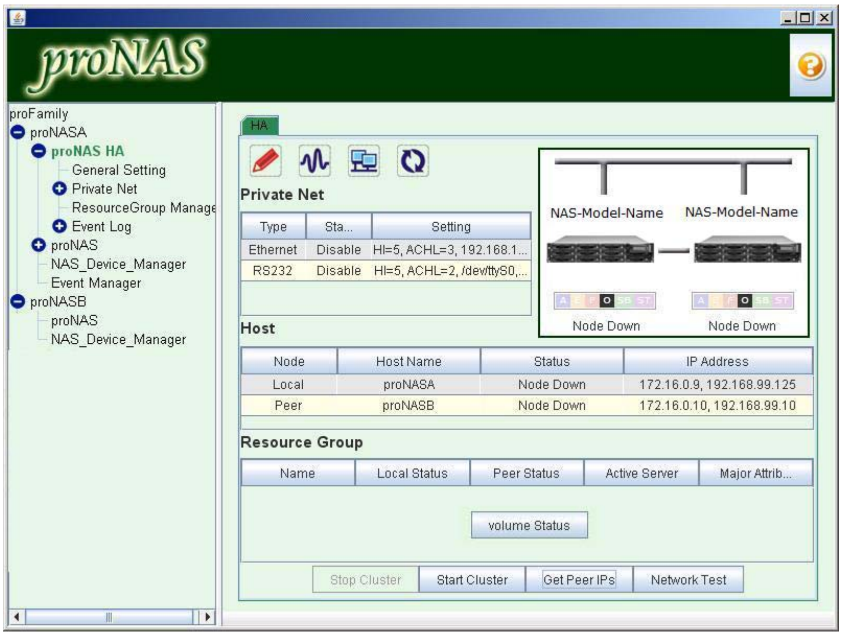
Preserved Days – Select the number of days that the log will be preserved before deleting.

Operational Preferences:

On Server Shutdown, failover the resource groups automatically – When enabled, the resource groups will be failed over to the other server when this server shutdown.

On Server Startup, start the cluster system automatically – When enabled, the cluster system will be started automatically when this server starts up.

7. Back to proNAS HA node, click "Get Peer IPs" button. The IP addresses of the peer server will then be displayed in the status info table. Be sure that it gets the peer IP addresses! If it fails, check again the hostname that you supplied in step 6.



Private Net

Type	Sta...	Setting
Ethernet	Disable	HI=5, ACHL=3, 192.168.1...
RS232	Disable	HI=5, ACHL=2, /dev/ttyS0,...

Host

Node	Host Name	Status	IP Address
Local	proNASA	Node Down	172.16.0.9, 192.168.99.125
Peer	proNASB	Node Down	172.16.0.10, 192.168.99.10

Resource Group

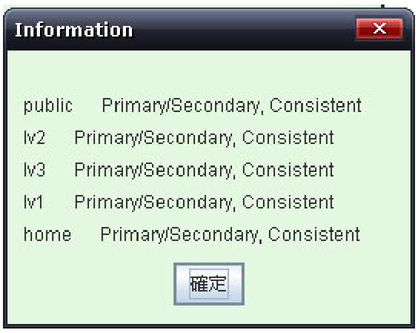
Name	Local Status	Peer Status	Active Server	Major Attrib...

Buttons:

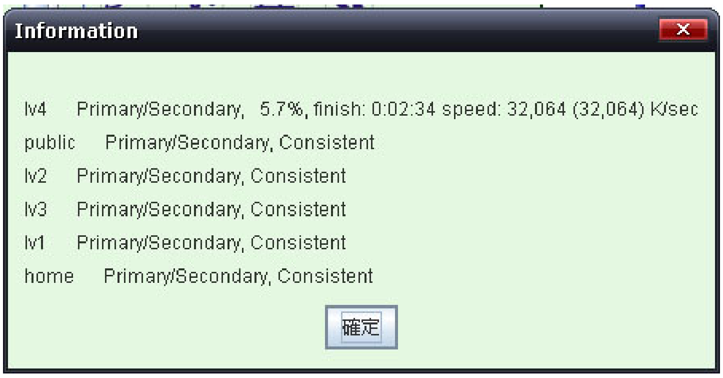
Stop Cluster	Stop Cluster Operation.
Start Cluster	Start Cluster Operation.
Get peer IPs	Get the IP's of the peer server and display it in the host peer table.
Network Test	Tool for testing network IP address (e.g ping ip)
Volume Status	Shows the current Replication status of logical volumes.

NOTE: When HA is already configured and Cluster is in operation, you can see the current replication status of logical volumes by clicking "Volume Status".

Volume Status Example 1: All logical volume Replications are consistent



public Primary/Secondary, Consistent
lv2 Primary/Secondary, Consistent
lv3 Primary/Secondary, Consistent
lv1 Primary/Secondary, Consistent
home Primary/Secondary, Consistent

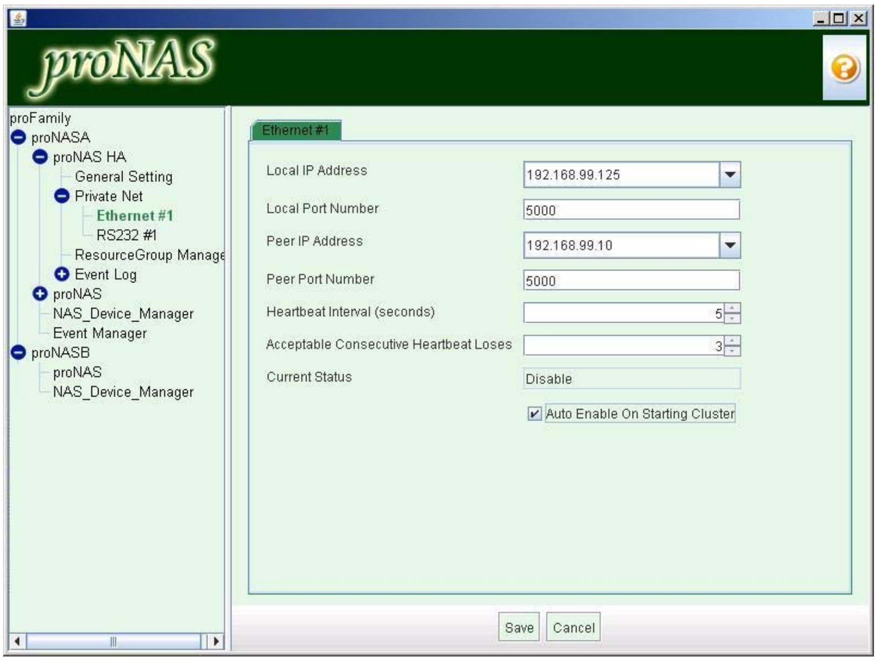


Volume Status Example 2: Replication of one logical volume is initializing.

Information

```
lv4     Primary/Secondary,   5.7%, finish: 0:02:34 speed: 32,064 (32,064) K/sec
public     Primary/Secondary, Consistent
lv2     Primary/Secondary, Consistent
lv3     Primary/Secondary, Consistent
lv1     Primary/Secondary, Consistent
home     Primary/Secondary, Consistent
```

8. Go to Private Net node down to "Ethernet#1". Set the local and peer IP address, check "Auto Enable on Starting Cluster" then save. Be sure not to select the public IP (eth0 IP address) for both proNAS box.



Local IP Address: 192.168.99.125
Local Port Number: 5000
Peer IP Address: 192.168.99.10
Peer Port Number: 5000
Heartbeat Interval (seconds): 5
Acceptable Consecutive Heartbeat Loses: 3
Current Status: Disable
☑ Auto Enable On Starting Cluster

Private Net: Ethernet

Local/peer Port Number	Specify an unused TCP port for each server to receive the heartbeat sent from the peer server. The default value is 5000.
Local/peer IP Address	Specify the IP Addresses of the network interface cards that constitutes both ends of the private net. These IP addresses must be on a separate subnet from the public net.
Heartbeat Interval	Specify the period of time between two consecutive heartbeats.
Acceptable Consecutive	Each server will keep counting and timing the heartbeats received from the peer server. If the number of times a

Heartbeat Loses	server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource group of the peer server will be taken over.
Auto enable on starting cluster	This option is disabled by default. This private net will be enabled automatically when starting cluster. Add the checkmark to enable this option.

9. Configure private net "RS232#1", if you setup serial port as an additional private net.

Private Net: RS232

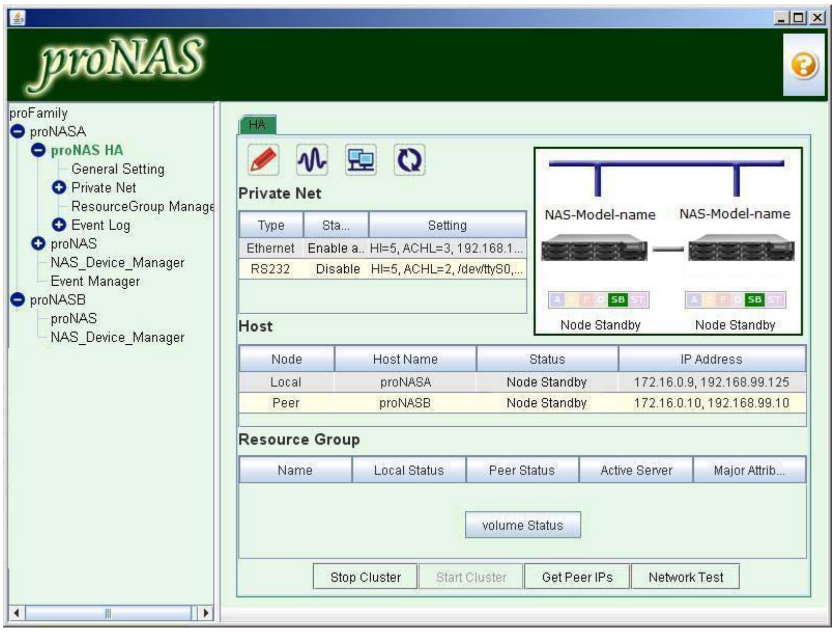
To use RS232 as a private net, you need to configure Serial ports settings in proNAS System Manager > Serial Ports tab, select either COM1 or COM2 for proNAS-HA.

Local Serial Port	Specify an unused serial port for each server to receive the heartbeat sent from the peer server.
Baud Rate	Specify the Baud Rate of the selected serial ports.
Heartbeat Interval	Specify the period of time between two consecutive heartbeats.
Acceptable Consecutive Heartbeat Loses	Each server will keep counting and timing the heartbeats received from the peer server. If the numbers of times a server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource groups of the peer server will be taken over.
Auto enable on starting cluster	This option is disabled by default. This private net will be enabled automatically on starting cluster. Users can add the checkmark to enable this option

10. Follow the same steps from step 5 to step 9 to configure your standby Backup Server except you need to select "**Standby(local host) – Active(peer-host) Mode**" as the Cluster Mode.

11. Click "Start Cluster" button.

12. Wait until the status of the local and peer server are in be standby-standby mode respectively. The statuses of the private net must also be "Enabled and Healthy". If this is not the output, check and repeat previous steps.



Private Net

Type	Sta...	Setting
Ethernet	Enable a..	HI=5, ACHL=3, 192.168.1...
RS232	Disable	HI=5, ACHL=2, /dev/ttyS0,...

Host

Node	Host Name	Status	IP Address
Local	proNASA	Node Standby	172.16.0.9, 192.168.99.125
Peer	proNASB	Node Standby	172.16.0.10, 192.168.99.10

Resource Group

Name	Local Status	Peer Status	Active Server	Major Attrib...

13. Go to "Resource Group Manager" then press "Add Resource Group".

The Resource Group Manager of proNAS HA is used to manage resource groups. Users need to configure resource groups only on one of the servers, usually the Active server. proNAS HA will automatically synchronize the status of resource groups between both servers. Note that users are prohibited to create or remove resource groups unless proNAS HA are running on both servers and at least one of the private net is functioning.

Buttons:

Add Resource Group button	Add new resource group member. User can specify the name of the resource group. This name must be unique for the resource groups within the cluster
Switch All Resource Groups from Peer	This is to manually takeover the all resource groups from the peer server. Users can manually takeover resource groups from the peer server to perform maintenance or troubleshooting on the active server. This button will be displayed only if resource groups are bring in.
Switch All Resource Groups to Peer	This is to manually failover the all resource groups to the peer server. Users can manually failover resource groups to the peer server to perform maintenance or troubleshooting on the active server. This button will be displayed only if resource groups are bring in.

14. Input a resource group name. You may check "Auto Switch back" or "Auto Bring In" then click “Save”.

Resource Group Properties:

Resource Name	A unique name for identifying the resource group
Active Server	The active server of the resource group
Backup Server	The peer server is automatically display
Local Status	The status of the local server
Peer Status	The status of the peer server
Auto-switch back	An option for enabling the Group to be switched back from the Backup server to the Target server automatically when the Target Server is available again.
Auto Bring In	An option for enabling the resource group to be brought in automatically when Cluster is started.

Buttons:

Bring in	The selected resource group will be activated and brought under the protection of proNAS HA. This button is only visible if there are resource group added.
Bring out	The selected resource group will be brought out from the protection of proNAS HA. A resource group can be brought out of cluster to perform maintenance or troubleshooting. This button is visible if resource groups are brought in.

15. Click the resource group name on the left tree node then press "Add Resource".

16. On the "Basic Settings" tab, input a resource name.

Resource Basic Setting:

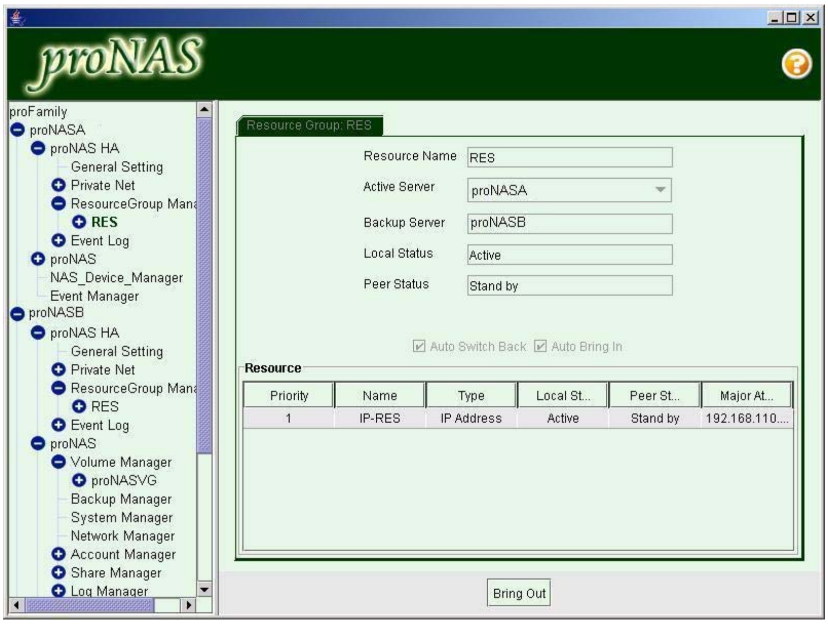
Resource Name	A unique name for identifying the resource group.
AC interval (Availability Check Interval)	A time interval for proNAS HA to check the availability of the resource group periodically.
AC Retry (Availability Check Retry)	The number of times for proNAS HA to check the availability of the resource group periodically.
Stop timeout	Specify the period of time for resource startup and stop. If a server fail to receive the heartbeat in time exceed this threshold, the peer server will be considered down or unavailable. The resource group of the peer server will be taken over.
Skippable if releasing resource fail	This option is disabled by default. Basically all of the resource group of the peer server will be taken over when the peer server fails. Users can add the checkmark to enable this option. The failover will be taken even if resource releases fail.

17. On the "IP Address Resource" tab, select the original IP address (eth0 IP) for both local and remote proNAS, enter an active IP address, active subnet mask and then save. Active IP address is the virtual IP address.

IP Resource:

Original IP Address	Choose the original IP Address for the local and peer server.
Active IP Address	Type an IP Address (virtual IP) for client-end applications to access specific resources on the NAS Target Server.
Active Subnet Mask	The subnet mask used by the Active IP Address.

18. Click the resource group name on the left tree node then press "Bring In". The resource name will be brought in.



Resource Name: RES

Active Server: proNASA

Backup Server: proNASB

Local Status: Active

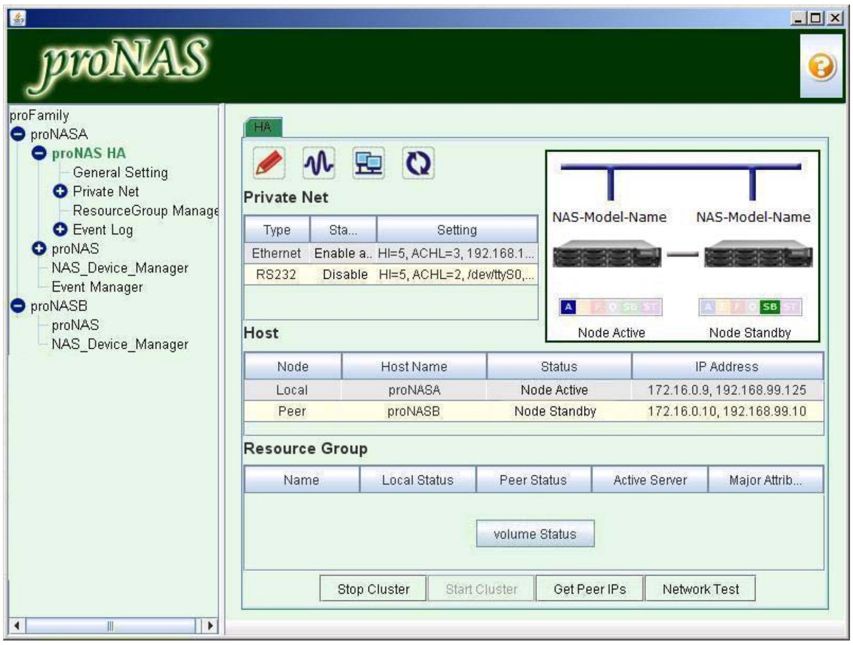
Peer Status: Stand by

☑ Auto Switch Back ☑ Auto Bring In

Resource

Priority	Name	Type	Local St...	Peer St...	Major At...
1	IP-RES	IP Address	Active	Stand by	192.168.110....

19. The Cluster Servers will be in Active – Standby mode.



Private Net

Type	Sta...	Setting
Ethernet	Enable a..	HI=5, ACHL=3, 192.168.1...
RS232	Disable	HI=5, ACHL=2, /dev/ttyS0,...

Host

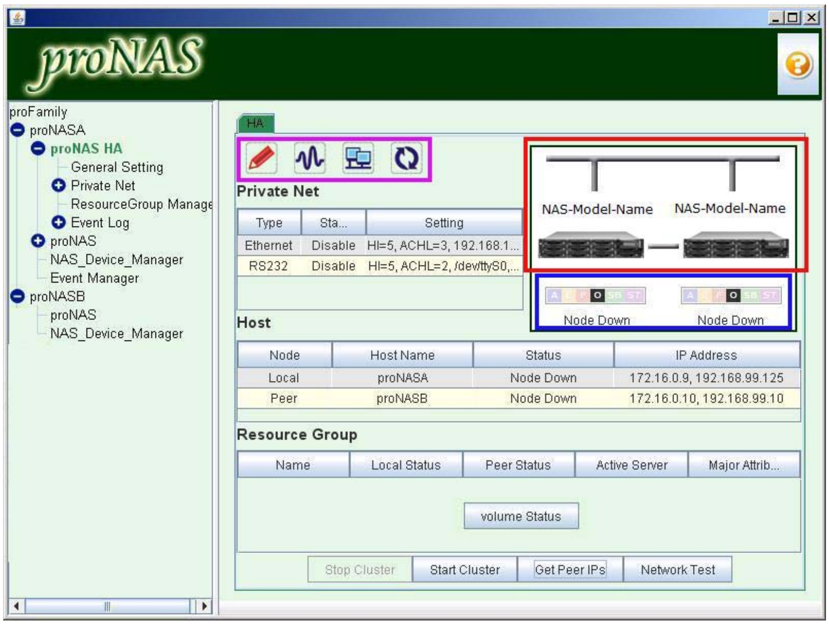
Node	Host Name	Status	IP Address
Local	proNASA	Node Active	172.16.0.9, 192.168.99.125
Peer	proNASB	Node Standby	172.16.0.10, 192.168.99.10

Resource Group

Name	Local Status	Peer Status	Active Server	Major Attrib...

8.3 ProNAS HA Properties

Status Properties



Private Net

Type	Sta...	Setting
Ethernet	Disable	HI=5, ACHL=3, 192.168.1...
RS232	Disable	HI=5, ACHL=2, /dev/ttyS0,...

Host

Node	Host Name	Status	IP Address
Local	proNASA	Node Down	172.16.0.9, 192.168.99.125
Peer	proNASB	Node Down	172.16.0.10, 192.168.99.10

Resource Group

Name	Local Status	Peer Status	Active Server	Major Attrib...

Users can monitor all the resources from the proNAS HA Status Pad. Users can monitor the status of the servers, the resource groups and the private net in real-time. The status after the Cluster Service starts running on both servers.

The status icons in status bar and their respective meaning:

A E F O SB ST - Active Mode

A **E** F O SB ST - Error Mode

A E **F** O SB ST - Fail Mode

A E F **O** SB ST - Offline Mode

A E F O **SB** ST - Standby Mode

A E F O SB **ST** - Startup Mode

The private net status:

The colored lines between the servers indicate the status of the private net. Also status is displayed in the function bar.

- **Gray line** Only one end of the Private Net is created, the other end is not yet created.
- **Red line** Both ends of the Private Net are established but either one of the servers cannot receive heartbeat message from the peer server.
- **Blue line** Both ends of the Private Net are established and both servers are exchanging heartbeat messages.

Indicators:

Users can accurately monitor the status of the system such as the License status, Private Net, Public Net and the resource takeover/failover. When a condition occurs, the icon will turn red. You will also see a message appear in the Event Log.

Private Net: This icon will turn red if there's a problem with the connection of the private net.

Public Net: This icon will turn red if there's a problem with the connection of the public net.

Failover/Takeover: This icon will turn red during the failover or takeover scenario.

License: This icon will turn red if proNAS HA is not registered.

Host box: Display the status of Local and Peer Server

Resource Group box: Display the resource group status

Buttons:

Stop Cluster button	Stop Cluster Operation.
Start Cluster button	Start Cluster Operation.
Get peer IPs button	Get the IP's of the peer server and display it in the host peer table.
Network test button	Tool for testing network IP address (e.g ping ip)

8.4 Extending a Logical Volume in HA

Extending a logical volume while in cluster is basically not allowed same as in replication, however here is the workaround.

1. Stop Cluster
2. Stop HA service for both proNAS.
3. Abort the replication of the logical volume that needs to be extended.
4. Extend the logical volume on the Active server.
5. Removed the logical volume (the replica) on the standby server.
6. Start HA service for both proNAS.
7. Start cluster.

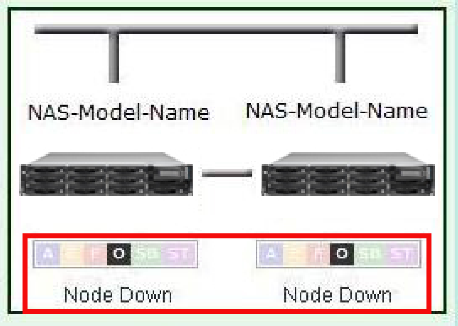
8.5 Clear All HA Configuration

A function button “Clear All HA Configuration” is provided to remove all proNAS HA configuration. This is located in General Setting tab.

When you clear the HA configuration, you have an option to clear all logical volume Replication. If you don’t clear the all Replication, only HA configuration will be reset, and all logical volumes will still have Replication.

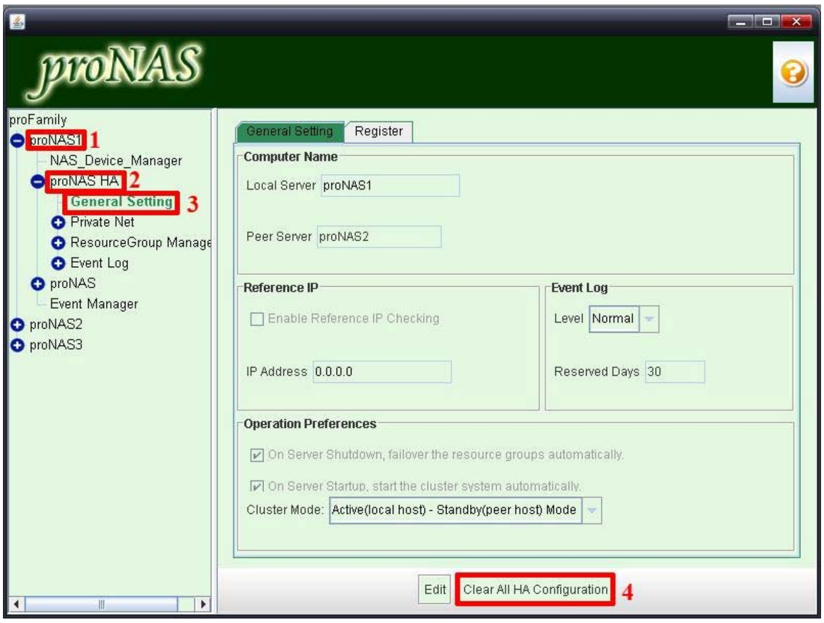
After you clear all HA configuration and clear all Replication, you can re-configure another HA. This is normally used when one of the proNAS servers has failed and you want to reconfigure HA for another (new) proNAS server using the remaining proNAS server.

IMPORTANT: Before you clear all HA configuration, make sure the cluster is stopped (all nodes are “down”).



To remove all existing proNAS HA configuration:

1. Select the proNAS node name, click proNAS HA, and select General Setting. Click “Clear All HA Configuration”.



Computer Name

Local Server proNAS1

Peer Server proNAS2

Reference IP

☐ Enable Reference IP Checking

IP Address 0.0.0.0

Event Log

Level Normal

Reserved Days 30

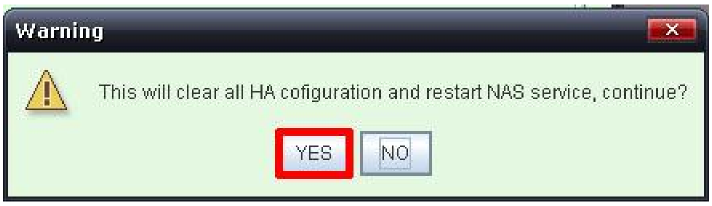
Operation Preferences

☑ On Server Shutdown, failover the resource groups automatically.

☑ On Server Startup, start the cluster system automatically.

Cluster Mode: Active(local host) - Standby(peer host) Mode

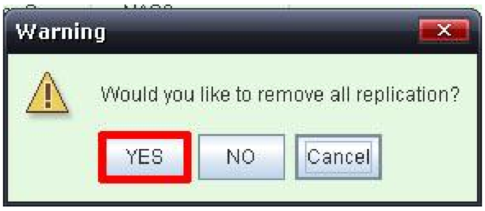
2. A warning message to clear all HA configuration will be displayed. Click “Yes” to proceed.



Warning

This will clear all HA cofiguration and restart NAS service, continue?

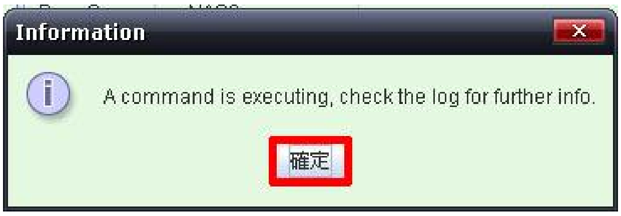
3. A warning message to remove all replication in logical volumes will be displayed. Click “Yes” to remove Replication in all logical volumes, or “No” to just clear HA but replication of logical volumes still exists.



Warning

Would you like to remove all replication?

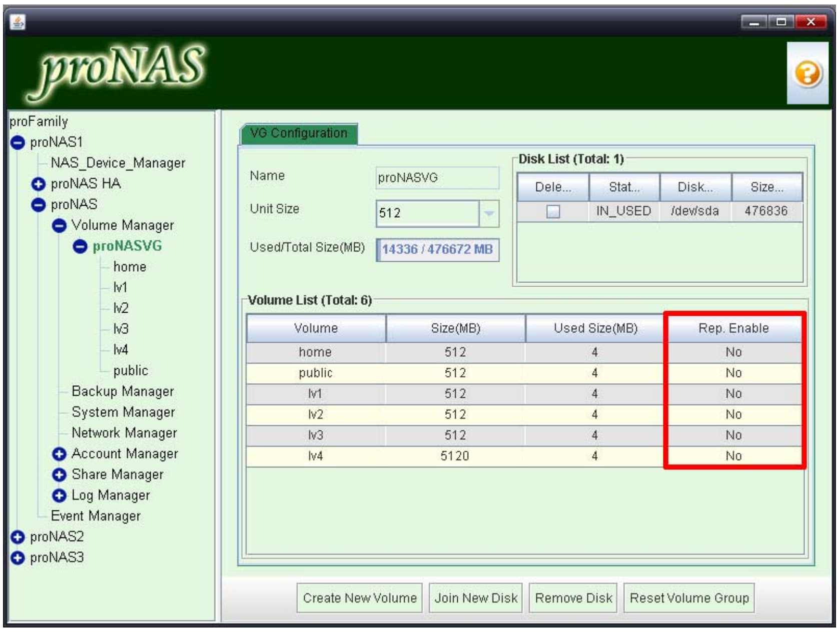
4. An information message will be displayed. Click “OK” to close the message. You can verify the proNAS HA Event Log for further information.



Information

A command is executing, check the log for further info.

Example of Replication status after selecting “**Yes**” to remove all replication:



Name: proNASVG

Unit Size: 512

Used/Total Size(MB): 14336 / 476672 MB

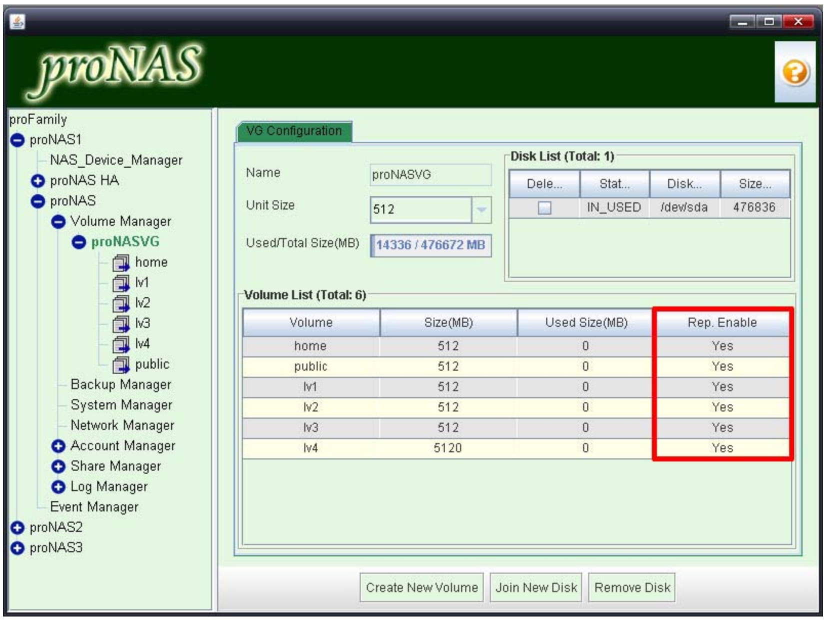
Disk List (Total: 1)

Dele...	Stat...	Disk...	Size...
□	IN_USED	/dev/sda	476836

Volume List (Total: 6)

Volume	Size(MB)	Used Size(MB)	Rep. Enable
home	512	4	No
public	512	4	No
lv1	512	4	No
lv2	512	4	No
lv3	512	4	No
lv4	5120	4	No

Example of Replication status after selecting “**No**” to retain all replication:



Name: proNASVG

Unit Size: 512

Used/Total Size(MB): 14336 / 476672 MB

Disk List (Total: 1)

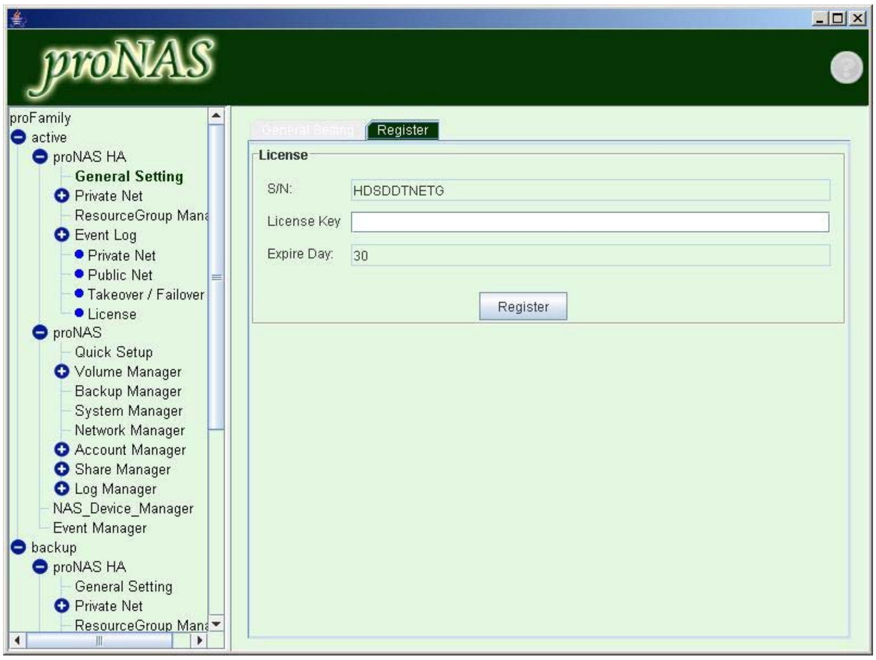
Dele...	Stat...	Disk...	Size...
□	IN_USED	/dev/sda	476836

Volume List (Total: 6)

Volume	Size(MB)	Used Size(MB)	Rep. Enable
home	512	0	Yes
public	512	0	Yes
lv1	512	0	Yes
lv2	512	0	Yes
lv3	512	0	Yes
lv4	5120	0	Yes

8.6 License Registration

To apply ProNAS HA license codes and register them to ProNAS HA users must first get the S/N of the two servers. Forward the S/N to your local ProNAS HA provider. Then Input the acquired License and click “Register” button. Users can now put ProNAS HA to work.



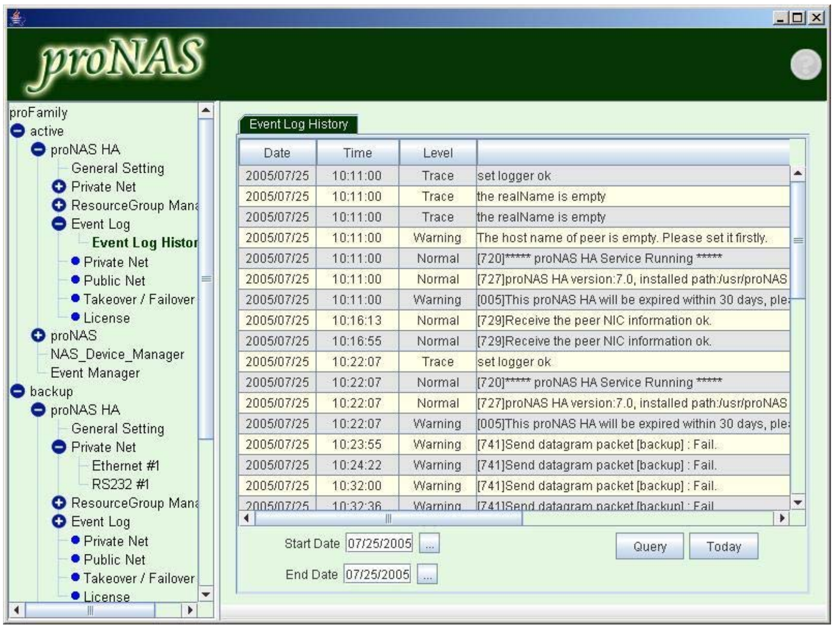
License

S/N: HDSDDTNETG

License Key:

Expire Day: 30

8.7 Event Log Properties



Date	Time	Level	
2005/07/25	10:11:00	Trace	set logger ok
2005/07/25	10:11:00	Trace	the realName is empty
2005/07/25	10:11:00	Trace	the realName is empty
2005/07/25	10:11:00	Warning	The host name of peer is empty. Please set it firstly.
2005/07/25	10:11:00	Normal	[720]***** proNAS HA Service Running *****
2005/07/25	10:11:00	Normal	[727]proNAS HA version:7.0, installed path:/usr/proNAS
2005/07/25	10:11:00	Warning	[005]This proNAS HA will be expired within 30 days, ple
2005/07/25	10:16:13	Normal	[729]Receive the peer NIC information ok.
2005/07/25	10:16:55	Normal	[729]Receive the peer NIC information ok.
2005/07/25	10:22:07	Trace	set logger ok
2005/07/25	10:22:07	Normal	[720]***** proNAS HA Service Running *****
2005/07/25	10:22:07	Normal	[727]proNAS HA version:7.0, installed path:/usr/proNAS
2005/07/25	10:22:07	Warning	[005]This proNAS HA will be expired within 30 days, ple
2005/07/25	10:23:55	Warning	[741]Send datagram packet [backup] : Fail.
2005/07/25	10:24:22	Warning	[741]Send datagram packet [backup] : Fail.
2005/07/25	10:32:00	Warning	[741]Send datagram packet [backup] : Fail.
2005/07/25	10:32:36	Warning	[741]Send datagram packet [backup] : Fail

Start Date 07/25/2005

End Date 07/25/2005

All the messages generated by ProNAS HA will be displayed in the Event Log. The messages can help users to identify the possible reasons that prevent ProNAS HA from operating normally.

APPENDIX

1. Upgrading Firmware of JBOD Controller SAS Expander

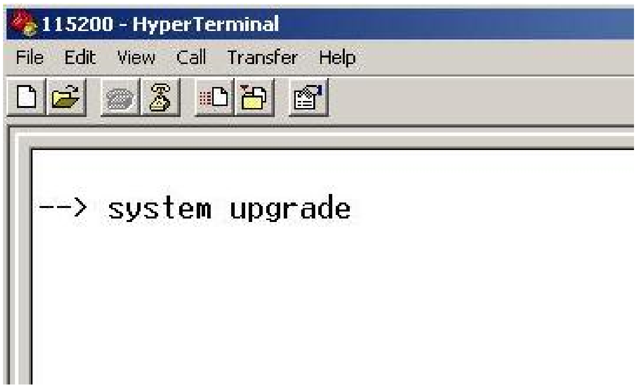
NOTE: The NAS system must be restarted and startup of OS must be suspended (hold off) by going into motherboard BIOS. After firmware upgrade, the NAS system can be started normally.

1. Connect RS232 null modem cable (Phone jack to DB9) from RS-232 Port (Phone jack) to serial port of PC or other host computer.

2. Setup terminal port settings as follows:

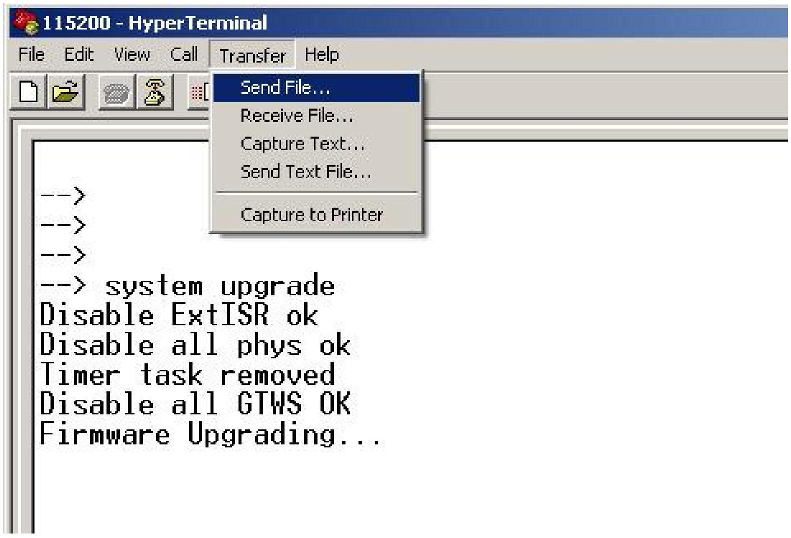
   Bits per second: 115200
   Data bits: 8
   Parity: None
   Stop bits: 1
   Flow Control: None

3. Open terminal session and press Enter key until the **-->** prompt appears. Type "**system upgrade"** and press Enter.



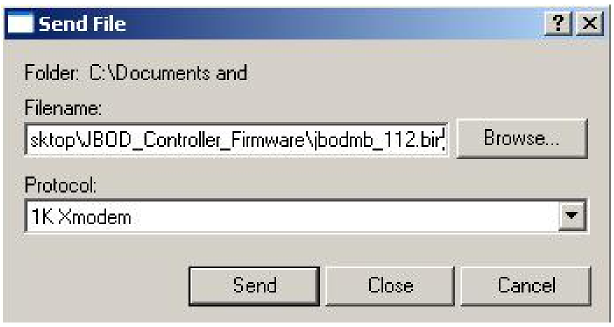
```
--> system upgrade
```

4. Select **Transfer** and **Send File…**.



```
-->
-->
-->
--> system upgrade
Disable ExtISR ok
Disable all phys ok
Timer task removed
Disable all GTWS OK
Firmware Upgrading...
```

5. Select the path where firmware file is located or saved. Set communication protocol to **1K Xmodem**, and click **Send**.

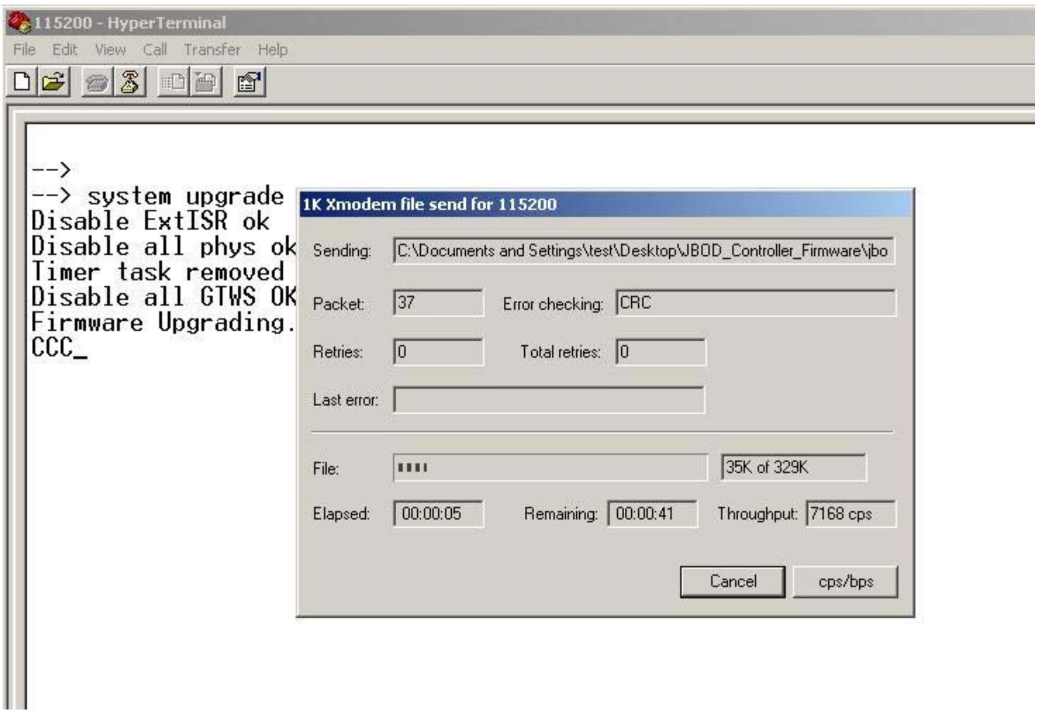


Folder: C:\Documents and

Filename: sktop\JBOD_Controller_Firmware\jbodmb_112.bin

Protocol: 1K Xmodem

6. Wait for file transfer to complete.


115200 - HyperTerminal
File Edit View Call Transfer Help
1K Xmodem file send for 115200
Cancel
cps/bps

```
-->
--> system upgrade
Disable ExtISR ok
Disable all phys ok
Timer task removed
Disable all GTWS OK
Firmware Upgrading.
CCC_
```

Sending: C:\Documents and Settings\test\Desktop\JBOD_Controller_Firmware\jbo

Packet: 37 Error checking: CRC

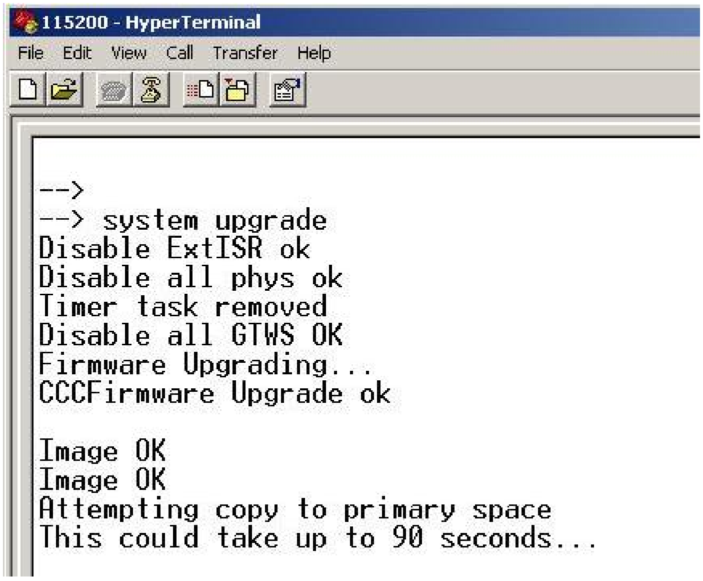
Retries: 0 Total retries: 0

Last error:

File: 35K of 329K

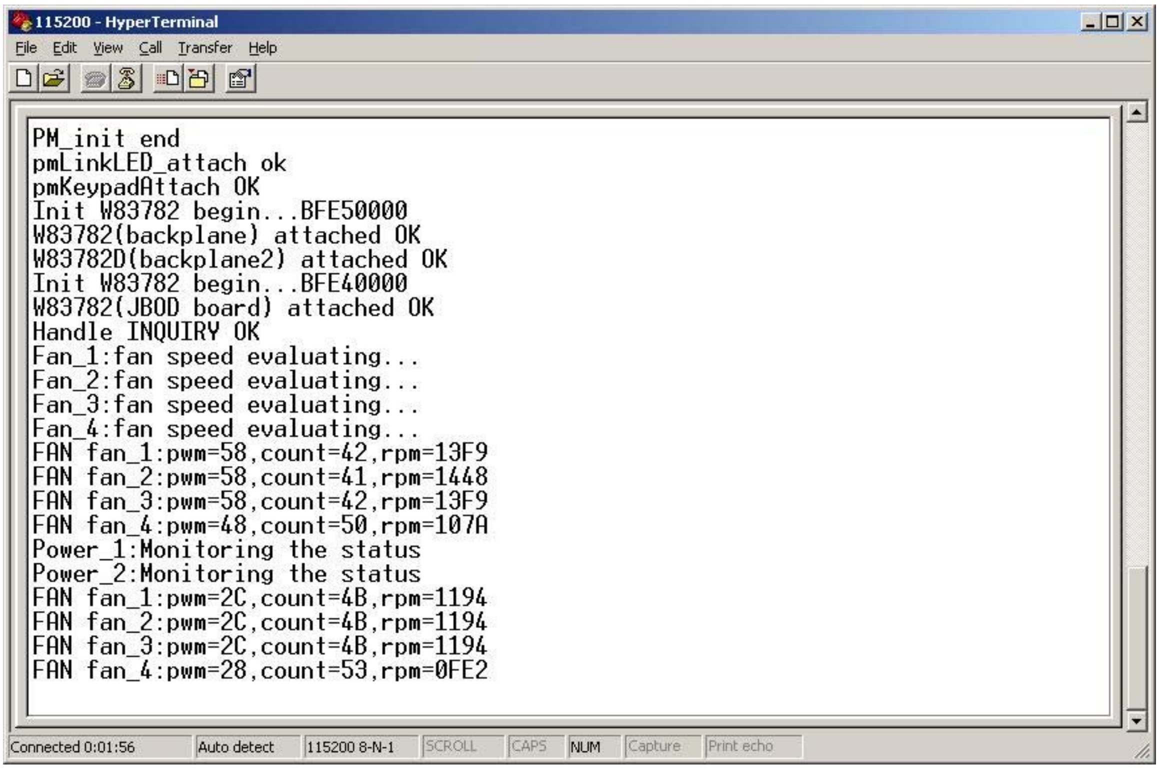
Elapsed: 00:00:05 Remaining: 00:00:41 Throughput: 7168 cps

7. When file transfer is completed, JBOD Controller will auto restart.



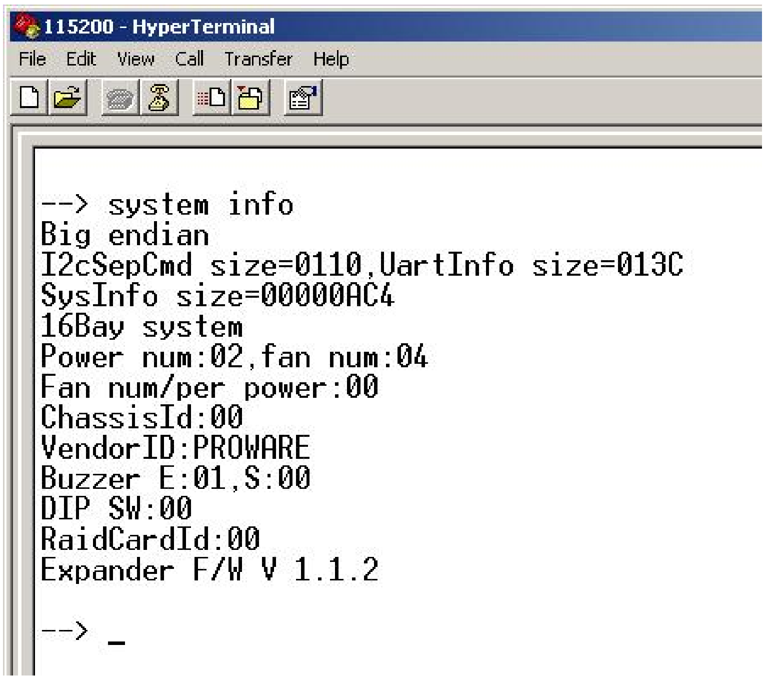
```
-->
--> system upgrade
Disable ExtISR ok
Disable all phys ok
Timer task removed
Disable all GTWS OK
Firmware Upgrading...
CCCFirmware Upgrade ok

Image OK
Image OK
Attempting copy to primary space
This could take up to 90 seconds...
```

8. Please power off then power on to make sure firmware update is complete.



```
PM_init end
pmLinkLED_attach ok
pmKeypadAttach OK
Init W83782 begin...BFE50000
W83782(backplane) attached OK
W83782D(backplane2) attached OK
Init W83782 begin...BFE40000
W83782(JBOD board) attached OK
Handle INQUIRY OK
Fan_1:fan speed evaluating...
Fan_2:fan speed evaluating...
Fan_3:fan speed evaluating...
Fan_4:fan speed evaluating...
FAN fan_1:pwm=58,count=42,rpm=13F9
FAN fan_2:pwm=58,count=41,rpm=1448
FAN fan_3:pwm=58,count=42,rpm=13F9
FAN fan_4:pwm=48,count=50,rpm=107A
Power_1:Monitoring the status
Power_2:Monitoring the status
FAN fan_1:pwm=2C,count=4B,rpm=1194
FAN fan_2:pwm=2C,count=4B,rpm=1194
FAN fan_3:pwm=2C,count=4B,rpm=1194
FAN fan_4:pwm=28,count=53,rpm=0FE2
```

9. In command line, type **system info** to verify SAS Expander firmware version.



```
--> system info
Big endian
I2cSepCmd size=0110,UartInfo size=013C
SysInfo size=00000AC4
16Bay system
Power num:02,fan num:04
Fan num/per power:00
ChassisId:00
VendorID:PROWARE
Buzzer E:01,S:00
DIP SW:00
RaidCardId:00
Expander F/W V 1.1.2

--> _
```

10. The NAS system can be started normally.